On forms of the affine line over a field

AUTHOR(S):

Kambayashi, Tatsuji; Miyanishi, Masayoshi

LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

10

ON FORMS OF THE AFFINE LINE OVER A FIELD

BY

TATSUJI KAMBAYASHI
and
MASAYOSHI MIYANISHI

Published by
KINOKUNIYA BOOK-STORE Co., Ltd.
Tokyo, Japan

LECTURES IN MATHEMATICS

Department of Mathematics

KYOTO UNIVERSITY

10

On forms of the affine line over a field

BY

Tatsuji Kambayashi

and

Masayoshi Miyanishi

Published by

KINOKUNIYA BOOK-SOTRE CO., Ltd.

Printed in Japan

Author's addresses

T. Kambayashi*

Department of Mathematics, Northern Illinois University
Dekalb, Illinois 60115, U.S.A.

M. Miyanishi

Department of Mathematics, Faculty of Science, Osaka University
Toyonaka, Osaka 560, JAPAN

* Supported in part by National Science Foundation under research grant MCS 72-05131.

CONTENTS

Introduction

An algebraic variety X defined over a field k is said to be a k-form of the n-dimensional affine space A^n if for a suitable algebraic extension field k' of k there exists a k'-isomorphism of X with A^n. In case such k' can be chosen to be separable or purely inseparable over k, the k-form X is called separable or purely inseparable, respectively. It has been known that for $n = 1$ or 2 all k-forms of A^n are purely inseparable In the present paper, we are concerned with the case $n = 1$ only, namely with the forms of the affine line A^1.

The earliest examples of purely inseparable forms of the affine line A^1 were constructed by Rosenlicht in his rationality papers [15, 16]; those were in fact forms of the one-dimensional vector group G_a. The line of investigation was taken up later by Russell in [17], in which among other things all forms of G_a were completely described. In section 6 of our joint monograph [8] with Takeuchi on unipotent algebraic groups we have obtained some further results. For example, we were able to determine all k-forms of A^1 of genus ≤ 1 carrying a k-rational point and to find some information about the Picard groups of certain forms of A^1.

The present paper is a natural sequel to the joint work [8] mentioned above, which will be referred to hereafter as KMT. We begin in Section 1 (§1) with birational considerations: the concept of height is introduced for both forms of A^1 and forms of the rational function field $k(t)$, and we give an explicit description of all algebraic function fields which are purely inseparable k-forms of $k(t)$. Utilizing this result, we go on to describe forms of A^1 of height 1, though the results here are rather incomplete.

In Section 2 (§2), we examine the hyperelliptic forms of A^1 and completely determine them in terms of their function fields. As it turns out, in the characteristic $p > 2$ case, there is only one type of such function fields, whereas if the characteristic $p = 2$ there are two distinct types of such function fields, and hence such forms of A^1. As a by-product, all forms of genus 2 are determined. These latest results, taken in conjunction with the previous results of Rosenlicht, Russell, Queen [10] and us, still leave a large unexplored part of the field of research on forms of A^1: there remain to investigate nonhyperelliptic forms of A^1 of genus > 2 possessing only finitely many automorphisms. As part of such further investigation, we study in Section 3 (§3) the automorphism group of k-form of A^1. We have shown, among other thing, that the group of k-automorphisms of a k-form of A^1, if finite, is a semidirect product of a group of roots of unity in k and an additive subgroup of k; that the quotient variety of a k-form of A^1 by a finite group of its k-automorphisms is again a k-form of A^1; and that in case $p > 2$ one can construct a k-form of A^1 with exactly m k-automorphisms for every given integer $m \geq 1$ provided $(p,m) = (p,m + 1) = 1$. Section 4 (§4) is devoted to the study of the Picard group of a k-form of A^1 and its relationship with heights and various allied invariants. Thus, if $X = \operatorname{Spec} A$ is a k-form of A^1 of positive genus and C is the k-normal completion of X, we have demonstrated that the exponent of Pic X (=C(A)) is precisely p^{λ}, $\lambda :=$ the height of X, while the exponent of the connected Picard scheme $\underline{\mathrm{Pic}}^0_{C/k}$ equals $p^{\lambda'}$, $\lambda' :=$ the height of the function field k(X) of X over k. The last fact is established by means of an analysis of the effect caused on $\underline{\mathrm{Pic}}^0_{C/k}$ by the Frobenius morphism of

C. The results in §4 include also a description of the connected Picard scheme above in terms of generalized Jacobian variety over the algebraic closure $\bar{k}$, an explicit description, over the original ground field k, of the connected Picard scheme associated with a specific type of k-form of A^1, and several others.

The methods employed in the present paper vary somewhat from section to section. Already in KMT, Frobenius morphisms and homomorphisms played a significant part; in §1 below, they play a crucial role, side by side with the classical algebraic function theory. In §2, the classical theory of blowing-up of singularities on a plane curve, appropriately modified to suit our purposes, is systematically applied for the analysis of singularities. Another technique found useful in KMT was that of purely inseparable descent of exponent p by means of derivations; the same plays an important role in §3 below. The last section (§4) draws heavily on the theory of Picard schemes as well as arguments involving Frobenius morphisms.

As noted already, the affine plane, too, has no nontrivial separable forms. This fact was recently established by one of the authors in [9] after Šafarevič's suggestions. On the other hand, research on purely inseparable forms of the affine plane has barely begun, despite its apparent importance due in part to connection with unirational affine surfaces. Let us note lastly that the absence of nontrivial separable forms of A^n for all $n \geq 3$ is generally conjectural as true but remains unestablished.

Acknowledgements

Peter Russell read a preliminary version of this paper with care and understanding, and offered his comments, criticism and suggestions. Those turned out to be of substantial benefit to the authors in writing up the present version. The authors wish to acknowledge their indebtedness to him. The more salient points among Professor Russell's many contributions to this work are the following: the proofs of Theorem 1.5.1 and Lemma 4.5.5 have been simplified to the present ones owing to his suggestions; his suggestion is responsible for Theorem 3.1.5, allowing us to strengthen Theorem 3.2.2; the invariants ε and η of 4.1 have been introduced following Russell's suggestion, and some of the results in Proposition 4.1 related to these numbers are due to him.

The bulk of the research for the present paper was done during the academic year 1974-75 while Miyanishi held a visiting appointment at Northern Illinois University. The authors are grateful to the University for making possible their close collaborations.

Throughout the period of preparation for this paper, Kambayashi was supported by a National Science Foundation research grant. The Foundation's support, which greatly facilitated the completion of the manuscript, is gratefully acknowledged. Finally, the authors wish to express their heartfelt thanks to Professors H. Matsumura and M. Nagata for providing the opportunity to publish this paper in the excellent Kyoto Lecture series.

0. Notations, Conventions and Basic Preliminary Facts.

Notations, conventions and terminology of the present paper follow closely those of KMT, and conform to the general current practice. Let it suffice, therefore, that we make a few additional notes below. We include in the notes brief mention of the elementary facts that we shall use later.

0.1. All (but a few specifically excepted) local rings appearing in this paper are one-dimensional geometric domains over some field containing the ground field. Let o be such a local ring over a field k. Then, o is said to be k-normal if it is integrally closed in its field of quotients; this is so if and only if o is regular in the usual sense. The ring is said to be smooth if $\bar{k} \underset{k}{\otimes} o$ is $\bar{k}$-normal, where $\bar{k}$ denotes always the algebraic closure of k. The smoothness of o is equivalent to o being geometrically regular. The ring o is said to be k-smoothable if the integral closure of o in its field of quotients is smooth. Finally, o is called singular if it is not smooth. Let now X be a k-curve, by which is understood a geometrically integral one-dimensional k-scheme; let P be a point on X, and call its local ring o, which is contained in the field of functions $k(X)$. We shall speak of P being k-normal, smooth, k-smoothable and singular according as o is. (As a matter of fact, we shall often neglect to distinguish between P and its local ring o.) The same goes for the places of $k(X)$, which we shall identify with the discrete valuation rings in $k(X)$ containing k and also with the points on a k-normal complete model of $k(X)$. A place is said to have a certain property if the corresponding valuation ring has the same property.

Let us recall here a limited version of the Jacobian Criterion as adapted to suit our purpose best: Let $X = \mathrm{Spec}\ k[x_1, \ldots, x_n]$ be an affine k-curve and (o, m) a local ring of a $\bar{k}$-valued point $P = (x_i = \xi_i \in \bar{k} : 1 \leq i \leq n)$. The Jacobian condition (J) states that there exist $n - 1$ polynomials $f_i(T_1, \ldots, T_n)$ for $1 \leq i \leq n - 1$ belonging to the defining ideal of X over k such that the rank of $(\partial f_i/\partial T_k)$ evaluated at $T_j = \xi_j$ $(1 \leq j \leq n)$ equals $n - 1$. Then, the following hold:

0.1.1. The local ring o is smooth if and only if (J) is satisfied. In particular, (J) implies k-normality of o.

0.1.2. If o is k-normal and o/m is separable over k, then (J) is satisfied.

For the proofs of these, consult for instance Samuel [19, Chap. II, §4].

0.2. Let X be a k-curve as defined just above. Then, the genus of the algebraic function field $k(X)/k$, as defined in the well-known manner ([1], [2]), will be called the k-genus of X. If X is in addition complete (proper) over k, the arithmetic k-genus of X is defined to be the dimension of the connected Picard schme $\mathrm{Pic}^0_{X/k}$, or equivalently the k-vector space dimension of $H^1(X, \mathcal{O}_X)$. (Cf. KMT - §6.) Thus, the k-genus of X agrees with the arithmetic k-genus of a complete k-normal model of $k(X)$.

Suppose now that an affine plane k-curve Y is given by the equation $f(x,y) = 0$ with an irreducible $f \in k[x,y]$. Let $F(x_0,x_1,x_2) = 0$ be the equation obtained by homogenizing $f(x,y) = 0$ in the classical fashion: $x_1/x_0 := x$, $x_2/x_0 := y$. Those points on the projective plane k-curve C

defined by $F(x_0,x_1,x_2) = 0$ which do not lie on Y will be referred to as the points at infinity of Y. Note, however, that these points depend upon the choice of f and are not invariant even under k-automorphisms of the affine plane containing Y.

Let Z be a complete k-curve which is locally planar, i.e., whose local rings all have maximal ideals with two or fewer generators. Let P be a k-rational point on Z and $(o,m = o\xi + o\eta)$ the local ring belonging to P. Thus, o may be viewed as the localization of $k[\xi, \eta]$ at the prime ideal (ξ, η). Let $\zeta := \eta/\xi \in k(Z)$, and consider the ring $k[\xi, \zeta]$ or $k[\eta, 1/\zeta]$ containing $k[\xi, \eta]$. Let $o^{(1)}, \ldots, o^{(r)}$ be the localizations of $k[\xi, \zeta]$ or $k[\eta, 1/\zeta]$ at each of the prime ideals lying above (ξ, η). From the set of all local rings constituting Z we remove o and adjoin $o^{(1)}, \ldots, o^{(r)}$. The resulting set is easily seen to have a natural structure of k-scheme, which is called the proper transform Z' of Z by the blowing-up centered at P. The proper transform Z' is again a complete, locally planar k-curve. The points $o^{(1)}, \ldots, o^{(r)}$, if distinct from o, are called infinitely near points in the first neighborhood of o. By induction, one defines infinitely near points in the n-th neighborhood of points on Z for each $n \geq 1$.

0.2.1. The arithmetic k-genus of Z' equals that of Z less $m(m - 1)/2$, where m denotes the multiplicity of P.

This fact is classically well-known, provided $k = \bar{k}$ (algebraic closure of k). The reader might consult Fulton [5;Chap. 7] for instance. The proof of 0.2.1 is easily reduced to the classical case by extension of the ground field to $\bar{k}$. By the same token, the following holds true:

0.2.2. Let $P_1, \ldots, P_n$ be the totality of non- k-normal, k-rational points lying on Z or infinitely near Z. Call $\mu_1, \ldots, \mu_n$ their respective multiplicities. Then,

$$(\text{k-genus of } Z) \leq (\text{arithmetic k-genus of } Z) - \sum_{i=1}^{n} \mu_i(\mu_i - 1)/2$$

The equality holds if and only if all non- k-normal points on Z or infinitely near Z are k-rational.

It is implicitly asserted here that, if Z' is the proper transform of Z, obtained by blowing up all of $P_1, \ldots, P_n$, the arithmetic k-genus of Z' is larger than or equal to that of k-normalization of Z, equal if and only if Z' is k-normal.

0.2.3. If Z is immersed in the projective plane P_k^2 as a k-closed subscheme of degree d, then the arithmetic k-genus of Z equals $(d - 1)(d - 2)/2$.

0.3. In the first part of KMT, we made effective use of Frobenius morphisms of k-algebras, k-schemes and k-group schemes. They are useful in the present paper, too, especially in §1 and §4 below. Referring the reader to KMT - 1.3 ff for basic facts and notations, we mention here only a few more facts: let A be an algebra (commutative with unit, as always) over a field k of characteristic $p > 0$. Let $A^{(p)} = (k,f) \otimes A$ with $f : A \longrightarrow A$ by $a \longmapsto a^p$, and denote the image $f(A)$ of f by A^p. Let F be the Frobenius k-homomorphism:

$$F : A^{(p)} \longrightarrow A \quad \text{by} \quad x \otimes_p a \longmapsto xa^p.$$

0.3.1. $A^{(p)}$ *is reduced if and only if* $k^{1/p} \otimes_k A$ *is reduced; when that is so,* F *is a* k*-algebra isomorphism of* $A^{(p)}$ *onto the* k*-subalgebra* $k[A^p]$ *of* A.

0.3.2. *Each property of* $A^{(p)}$ *as* k*-algebra (e.g.,* k*-normal,* k*-regular,* k*-isomorphic with* $k[t]$*) is equivalent to the corresponding property of* $k^{1/p} \otimes_k A$ *as* $k^{1/p}$*-algebra.*

The proof of 0.3.1 is straightforward. The proposition 0.3.2 follows from the canonical equivalence between the category of k-algebras and that of $k^{1/p}$-algebras, resulting from the isomorphism $k^{1/p} \simeq k$ *via* $x \longmapsto x^p$. As a consequence of these two propositions, we have

0.3.3. *If there is a* $k^{1/p}$*-isomorphism* $k^{1/p} \otimes A \simeq k^{1/p}[t]$ *or* $k^{1/p} \otimes A \simeq k^{1/p}(t)$, *then there is a* k*-isomorphism* $k[A^p] \simeq k[u]$ *or* $k[A^p] \simeq k(u)$, *respectively; and vice versa provided* $k^{1/p} \otimes A$ *is reduced. (Here,* t *and* u *denote indeterminates.)*

0.4. *From now on until the end of the paper, we shall work over a fixed field* k, *nonperfect of characteristic* p. We shall denote by $\bar{k}$ and k_s respectively the algebraic closure and the separable closure of k. Sometimes the separable closedness of k ($k = k_s$) is assumed in order to avail oneself of a k-rational point; in a few instances the assumption is needed to provide for a dense subset of k-rational points. In those cases, the assumption is for a mere technical convenience and one can either substitute for it a milder assumption or otherwise modify the statement of the result suitably so as to preserve its validity. In other cases (notable in §2), however, the assumption $k = k_s$ plays an essential role as one draws upon the fact that the only irreducible monic polynomials over such a field k are of the type

$t^{p(\nu)} - a$ ($\nu \geq 0$, $a \in k$; $a \notin k^p$ if $\nu > 0$). Here as everywhere else in this paper, we denote by $X^{p(\nu)}$ the p^ν-th power of the entity X for any integer ν.

0.5. In regard to all of the terms defined in 0.1 through 0.3 and also to any schemes, morphisms, tensor products and fibre products, we shall as a rule omit the reference to the base field (or the base scheme) if it is k (or Spec k) as specified in 0.4, and if there is no danger of confusion.

1. Forms of the rational function field; forms of height one

1.1. Let X be a k-scheme such that $X \otimes \overline{k}$ is $\overline{k}$-isomorphic to the affine line $A^1_{\overline{k}} = A^1_k \otimes \overline{k}$. Such an X is called a k-form of the affine line A^1. When X is such, one can readily find a finite normal extension field k' over k such that $X \otimes k' \simeq A^1_{k'}$. Let k'' be the subfield of fixed elements under the automorphism group of k'/k; then the extensions k'/k'', k''/k are finite separable and finite purely inseparable, respectively. Since $(X \otimes k'') \otimes_{k''} k' \simeq X \otimes k' \simeq A^1_{k'}$, it follows that $X \otimes k'' \simeq A^1_{k''}$, as is well-known ([17], [21]). Thus, each k-form X of A^1 becomes $k^{p(-\nu)}$-isomorphic to $A^1 \otimes k^{p(-\nu)}$ after suitable base extension $k \longleftrightarrow k^{p(-\nu)}$, and the least $\nu \geq 0$ for which this happens will be called the height of k-form X.

Notation: $\nu = \mathrm{ht}(X)$. A k-form X of A^1 of height 0 is called trivial; X is then k-isomorphic to A^1, and vice versa. As a consequence of the definition, a k-form of A^1 is a geometrically integral smooth affine k-scheme of dimension 1, or a smooth affine k-curve as defined in 0.1.

1.2. Let K be an algebraic function field of one variable containing k as its field of constants. K is said to be a k-form of the rational function field $k(t)$ if a $\overline{k}$-isomorphism.

$$\overline{k} \otimes K \simeq \overline{k} \otimes k(t) = \overline{k}(t)$$

exists. The definition implies that K is necessarily a regular extension of k in Weil's sense. Let k' be a finite normal extension of k such that

$k' \otimes K \simeq k'(t)$, and let k'' be the fixed field of the automorphism group of k'/k. Then, $k' \otimes_{k''} (k'' \otimes K) \simeq k'(t)$ with k'/k'' finite separable, so that $k'' \otimes K$ is of genus zero. As well-known, $k'' \otimes K$ then must be k''-isomorphic to either a rational function field $k''(t)$ or a function field of a conic without k''-rational point. (Cf. [1;XVI, §4, pp. 302 ff].) We shall here concern ourselves only with the former case, of purely inseparable k-forms of $k(t)$, as these are the ones that occur as function fields of k-forms of A^1. Thus, let K be such that $k'' \otimes K \simeq k''(t)$ with k''/k finite purely inseparable. The height of such field K is defined to be the least natural number λ such that an isomorphism

$$k^{p(-\lambda)} \otimes K \simeq k^{p(-\lambda)} \otimes k(t)$$

exists over $k^{p(-\lambda)}$. We denote $\lambda = ht(K)$. Again, $\lambda = 0$ if and only if $K \simeq k(t)$, in which case the k-form K is called trivial.

1.3. If X is a k-form of A^1, its function field $k(X)$ is a k-form of $k(t)$. Note that

$$ht(X) \geq ht(k(X)),$$

but they do not always equal each other, as witnessed by the existence of non-trivial k-forms of A^1 whose function fields are rational over k. [See KMT - 6.8.1; also see §4 of this paper for detailed discussion of relations between $ht(X)$ and $ht(k(X))$.]

1.4. Let K be a purely inseparable k-form of $k(t)$, and let C be a complete k-normal model of K, uniquely determined up to k-isomorphisms.

Then, K is the function field of a k-form of A^1 if and only if C has at most one singular point. (N.B.: "singular" = "not smooth" = "not geometrically regular"; cf. 0.1 above.) In case C has a unique singular point P_∞, $X := C - P_\infty$ gives a non-trivial k-form of A^1 (cf. KMT - 6.7 ff). In case C is smooth, C is k-isomorphic to P^1_k except possibly when $p = 2$ (cf. KMT - 6.7.7); if P_∞ is any point purely inseparable over k on such C, $X := C - P_\infty$ gives a non-trivial k-form of A^1 again. Since k-rational non-trivial k-forms of A^1 have been completely classified (cf. KMT - 6.8.1), we consider only irrational k-forms of A^1 in this section (§1).

1.5. We shall now examine k-forms of the rational function field $k(t)$.

1.5.1. THEOREM. *Let K be a purely inseparable k-form of the rational function field $k(t)$, of height λ. Then, K is k-isomorphic to the function field of an affine plane k-curve defined by an equation of the type*

$$y^{p(\lambda)} = P(x) \quad \text{with} \quad P(x) \in k[x] \tag{1}$$

where $P(x) \notin k^p[x]$ and $P(x)$ has only simple factors over $\bar{k}$.

PROOF. By 0.3.3, we have $k[K^{p(\lambda)}] = k(x)$ for some $x \in K$, which implies that K is purely inseparable over $k(x)$. Take on the other hand a separating transcendence base of K/k, say $\{y\}$. Then, K is both separable and purely inseparable over $k(x,y)$, hence $K = k(x,y)$ and $y^{p(\lambda)} = f(x)/g(x) \in k(x)$. But $(yg(x))^{p(\lambda)} = f(x)g(x)^{p(\lambda)-1}$ and $k(x,y) = k(x,yg(x))$. Consequently, replacing y by $yg(x)$ which we anew call y, we have

$$y^{p(\lambda)} = P(x) \in k[x], \quad K = k(x,y) \tag{1'}$$

Since K/k is a regular extension, clearly $P(x) \in k[x^p]$ would be absurd. So, the derivative $P'(x)$ is nonzero. As we are free to substitute $y + a$ for y and $P(x) + a^{p(\lambda)}$ for $P(x)$ in (1'), we may arrange so that $P(x)$ and $P'(x)$ share no root in $\overline{k}$. Therefore, we may assume at our convenience that $P(x)$ has no multiple factors over $\overline{k}$. Finally, the fact that $P(x) \notin k^p[x]$ follows from the result 1.5.3 below.

1.5.2. COROLLARY. (a) Let K be a purely inseparable k-form of $k(t)$. Then, among the fields K', $k \subseteq K' \subseteq K$, such that $K' \simeq k(t)$ and K/K' purely inseparable, there exists a unique maximal one (which is $k(x)$ in the notation of 1.5.1).

(b) Let $X = \operatorname{Spec} A$ be a k-form of A^1. Then, among the k-algebras A', $k \subseteq A' \subseteq A$ such that $A' \simeq k[t]$ and A'/A purely inseparable, there exists a unique maximal one.

The proposition is essentially contained in Russell [17; LEMMA 1.3, p. 529]. However, we shall quickly draw it as a corollary to 1.5.1:

Proof: (a) Let K' be as above with $[K : K'] = p^\alpha$. Then, $k[K^{p(\alpha)}] \subseteq K' \simeq k(t)$, so by 0.3.3 and Lüroth's Theorem one gets $k^{p(-\alpha)} \otimes K \simeq k^{p(-\alpha)}(t)$. Hence, $\alpha \geq \lambda = ht(K)$. But $k[K^{p(\lambda)}] = k(x^{p(\lambda)}, P(x)) = k(x)$ (cf. 1.5.1), so $k[K^{p(\alpha)}] = k(x^{p(\alpha-\lambda)})$. Thus, $[K:k[K^{p(\alpha)}]] = [K : k(x)][k(x) : k(x^{p(\alpha-\lambda)})] = p^\lambda \cdot p^{\alpha-\lambda} = p^\alpha$, and $K' = k[K^{p(\alpha)}] \subseteq k(x)$ follows.

(b) Let $K = k(X)$ be the quotient field of A, and K' that of A'.

Let $\{o_i : i \in I\}$ be the totality of places of K finite on A. Then, A' is determined by K' as $A' = \bigcap_i (o_i \cap K')$. Noting $K' = k(x^{p(\delta)})$ for some $\delta \geq 0$, take the smallest $\delta \geq 0$ for which $\bigcap_i (o_i \cap k(x^{p(\delta)})) \simeq k[t]$ holds. Then, clearly, $A' \subseteq \bigcap_i (o_i \cap k(x^{p(\delta)})) = k[A^{p(\lambda+\delta)}] \simeq k[t]$, and $k[A^{p(\lambda+\delta)}]$ is the maximal subring sought, with $\lambda + \delta = ht(X)$. Q.E.D.

1.5.3. PROPOSITION. Let K be the function field of a plane k-curve defined by an equation of the type

$$y^{p(\lambda)} = f(x) \; ; \; f(x) \in k^{p(i)}[x], \quad f(x) \notin k^{p(i+1)}[x], \quad i \geq 0. \tag{2}$$

Then, K is a k-form of the rational function field $k(t)$ of height $\leq \lambda - i$.

Proof. Considering x and y as elements of Weil's universal domain containing k, we put $u := x^{p(-\lambda)}$. Then, we can rewrite (2) as

$$y^{p(\lambda)} = (f^{p(-\lambda)}(u))^{p(\lambda)}$$

or $y = f^{p(-\lambda)}(u) \in k^{p(-\lambda+i)}[u]$. This shows that $k^{p(-\lambda+i)} \otimes K$ is $k^{p(-\lambda+i)}$-isomorphic to a subfield of $k^{p(-\lambda+i)}(u,y) = k^{p(-\lambda+i)}(u)$, hence by Lüroth's Theorem $k^{p(-\lambda+i)} \otimes K \simeq k^{p(-\lambda+i)}(t')$ for some variable t' over $k^{p(-\lambda+i)}$. Q.E.D.

1.5.4. PROPOSITION. The affine plane curve X defined by an equation

$$y^{p(\lambda)} = P(x) \quad (P(x) \in k[x])$$

has only one place at infinity.

Proof. Let $A = k[x,y]/(y^{p(\lambda)} - P(x))$, and let $A' := k' \otimes_k A$ with $k' := k^{p(-\lambda)}$. Then A' is identified with a k'-subalgebra of $k'[u]$, if we put $x := u^{p(\lambda)}$ and $y := P^{p(-\lambda)}(u)$. Since $k'[u]$ is integral over A', Spec $A' = X \otimes k'$ has only one place at infinity. Since k' is purely inseparable over k, X has only one place at infinity.

1.6. Let K be an algebraic function field of one variable over k, and let o be a valuation ring of K corresponding to a point P on the complete k-normal model of K/k. In this subsection, we are concerned with the conditions for o (or P) to be smooth over k.

1.6.1. PROPOSITION. The following statements are equivalent to each other:

(i) o is smooth (= geometrically regular);

(ii) $k^{p(-1)} \otimes o$ is $k^{p(-1)}$-normal;

(iii) $k[o^p]$ is k-normal;

(iv) $k[o^p] = o \cap k[K^p]$.

Proof. (i)$\Leftrightarrow$(ii) : See EGA - IV, (22.5.8). (ii)$\Leftrightarrow$(iii) : By 0.3.1-2 above. (iii)$\Leftrightarrow$(iv) : Because $k[o^p]$ is in any event a one-dimensional local ring and $k[K^p]$ is a field.

1.6.2. An obvious but useful point: Let $o_0 := o \cap k[K^p]$; then, 1.6.1 - (iv) occurs if and only if the local ring $k[o^p]$ has the same residue class field as o_0 and contains a prime element of the valuation ring o_0. Another useful fact is that if o is k-rational, i.e., if the residue class field of o is k, then o is geometrically regular. This follows from the Jacobian criterion (cf. 0.1.2).

1.6.3. Let K, o and $o_0 = o \cap k[K^p]$ be as above. Let m, m_0 be the maximal ideals of o, o_0, respectively, and put $k := o/m$, $k_0 := o_0/m_0$. As is customary, $e(o_1:o_2)$ and $f(o_1:o_2)$ denote respectively the ramification index and the relative degree of a valuation ring o_1 dominating another one, o_2.

1.6.3.1. LEMMA. (a) If $k_0 = k$ and $f := f(o:o_0) = 1$, then o is smooth. (b) If $k_0 \supset k$ and $f = 1$, then o is not smooth (= singular).

Proof. (a) In this case, obviously $k = k$, too, and the second remark in 1.6.2 applies. (b) One can readily see that the residue field of the local ring $k[o^p]$ is $k[k^p]$, which in this instance is identical with $k[k_0^p]$. Clearly $k[k_0^p] \subset k_0$, so that $k[o^p] \subset o_0$ and o is not smooth by 1.6.1.

1.7. Let K, o be as in 1.6, and $o_0 = o \cap k[K^p]$. We now impose an additional condition that $K = k(x,y)$, function field of a plane k-curve

$$y^p = a_0 + a_1x + \ldots + a_nx^n = P(x) \tag{3}$$

where $P(x) \in k[x]$. By 1.5.2, K is a k-form of $k(t)$ of height ≤ 1, and $k[K^p] = k(x)$. We continue study of smoothness conditions for o under this additional hypothesis.

1.7.1. LEMMA. Assume that $k = k_s$ and o_0 is non- k-rational, i.e., $k_0 \supset k$. Then, o is smooth if and only if $e := e(o:o_0) = 1$.

Proof: If o is smooth, then $f \neq 1$ by 1.6.3.1 (b) so that $f = p$ and $e = 1$. As for the converse, as o_0 is realized as a localization of $k[x]$ at a prime of the type $(x^{p(\nu)} - d)$ with $d \in k - k^p$, $\nu > 0$, it is seen that

the prime element $x^{p(v)} - d$ of o_0 belongs to $k[o^p]$; hence, by 1.6.2, o is smooth if and only if $k[o^p]$ has the same residue field as o_0 has, i.e., if and only if $k[k^p] = k[d^{p(-v)}]$. This last holds in the case at hand because $e = 1$, $f = [k:k_0] = p$.

1.7.2. COROLLARY. If in (3) $P(x)$ is divisible by $x^{p(h)} - c$ but not by $(x^{p(h)} - c)^p$, where $h > 0$ and $c \in k - k^p$, then the point $(x = c^{p(-h)}, y = 0)$ on the curve $y^p = P(x)$ is not k-smoothable.

Proof. Clearly, we may assume $k = k_s$. Call o_0 the localization of $k[x]$ by $(x^{p(h)} - c)$. Then the unique extension of this valuation ring to $K = k(x,y)$ is the normalization of the local ring at $(x = c^{p(-h)}, y = 0)$. Call the extension o, its valuation function v. Then, $v(y^p) = p \cdot v(y) =$ (the multiplicity of $x^{p(h)} - c$ in $P(x)$) $\times v(x^{p(h)} - c)$. Since the first factor of the right side is not divisible by p, the second must be, and $e = v(x^{p(h)} - c) = p$ follows. By 1.7.1, then o is singular. Q.E.D.

Next, we consider the case of the k-rational o_0.

1.7.3. LEMMA. Assume that $o_0 = k[x]_{(x-c)}$ for some $c \in k$. Then, o is singular if and only if $P'(c) = 0$ and $P(c) \notin k^p$.

Proof. (only if) If $P'(c) \neq 0$ then o is smooth by Jacobian criterion. If $P'(c) = 0$ but $P(c) = d^p$ with $d \in k$, then one can rewrite (3) as

$$y^p - d^p = (x - c)^m Q(x)$$

for some $Q(x) \in k[x]$ and $m > 1$. The place o is determined by the point $(x = c, y = d)$ on the plane curve (3). Through the usual change of

variables, we may assume without loss that $1 < m < p$. Then, solve the congruence equation $mX \equiv 1 \pmod{p}$ and take a solution $X = s > 0$. Then, $ms - 1 = pt$ with $t > 0$, or $ms - pt = 1$. Thus, the element $(y - d)^{ps}/(x - c)^{pt}$ belongs to $k[o^p]$ and its order under the valuation o_0 is 1. Hence, $k[o^p]$ contains a prime element of o_0, and therefore o is smooth by 1.6.2.

(if): In this case, we have as our equation

$$y^p - d = (x - c)^m g(x)$$

with $1 < m$, $g(c) \neq 0$, $d \in k - k^p$, and o is the k-normalization of the local ring of the plane k-curve at hand at the point $(x = c, y = d^{1/p})$. Because the said local ring is evidently $k[x,y]_{(x-c)}$, it is already k-normal and hence agrees with o. If o were smooth, $k^{1/p} \otimes o = k^{1/p} \otimes k[x,y]_{(x-c)}$ should be $k^{1/p}$-normal, which it is not as seen by the Jacobian criterion. Therefore, o is singular. Q.E.D.

We next move to the place at infinity.

1.7.4. LEMMA. Let K be the function field of the affine plane k-curve defined by (3) subject to the condition that $a_n \neq 0$ and if $p|n$ then $a_n \notin k^p$. Then, the unique place $o \subset K$ at infinity of the plane curve is singular if and only if $p|n$ and $a_{n-1} = 0$.

Proof. Let us begin by remarking that the condition that $p|n$ entails $a_n \notin k^p$ is no real restriction at all, since if $p|n$ and $a_n = b^p$ $(b \in k)$ then y may be replaced by $z := y - bx^{n/p}$.

We now prove the 'if' part: Suppose thus $n = pr$. Then, if one puts

$w := y/x^r$, $z := 1/x$, one gets

$$w^p = a_n + a_{n-2}z^2 + \ldots + a_1 z^{n-1} + a_0 z^n, \qquad (4)$$

$k(x,y) = k(z,w)$, and o is the local ring of the plane curve (4) at $z = 0$, $w = a_n^{p(-1)}$. We know such o to be singular from 1.7.3.

As for the 'only if' part, first suppose $p|n$, $a_{n-1} \neq 0$. Then, using the same z, w as above, one obtains a plane curve birationally equivalent to the original curve given by

$$w^p = a_n + a_{n-1}z + \ldots + a_1 z^{n-1} + a_0 z^n \quad (a_{n-1} \neq 0)$$

which, in fact, is smooth at $(z = 0, w = a_n^{p(-1)})$. Hence, o is smooth. Next suppose $p\not|n$. Write $n = pr - s$, $r > 0$, $0 < s < p$. Then, by setting $w := y/x^r$, $z := 1/x$, one gets a k-birationally equivalent curve

$$w^p = z^s(a_n + a_{n-1}z + \ldots + a_1 z^{n-1} + a_0 z^n),$$

and o is the k-normalization of its local ring at $(z = 0, w = 0)$. By 1.7.3, o is then smooth. Q.E.D.

1.8. We now apply the foregoing results to describe the function fields of the k-forms of A^1 of height 1 as closely as we can. We may start out with a plane curve

$$y^p = a_0 + a_1 x + \ldots + a_n x^n = P(x) \in k[x]. \qquad (5)$$

Without loss of generality we may and shall assume that (i) $P(x)$ has simple roots only (cf. 1.5.1) and (ii) the highest nonzero coefficient a_n is a

non- p-th power in k in case $p|n$ (cf. proof of 1.7.4).

In view of the observation made in 1.4, the function field $K = k(x,y)$ of (5) gives a nontrivial k-form of A^1 if and only if K has a unique singular place. We examine when this is so, as follows:

First, the case $p|n$, $a_{n-1} = 0$. Then, by 1.7.4, the place at infinity is singular, so all places at finite distance must be smooth, or equivalently all points of the affine plane curve (5) must be k-smoothable. Let $q = (x = c \in \overline{k},\ y = P(c)^{1/p} \in \overline{k})$ be a point on the curve. If $P'(c) \neq 0$, then q is smooth. If $P'(c) = 0$ and $c \in k_s$, then according to 1.7.3 q is smooth if and only if $P(c) \in k_s^p$ ($\Leftrightarrow q$ is k_s-rational). If $P'(c) = 0$ and $c \notin k_s$, then a criterion of k-smoothability for q is provided by 1.6.3.1 (b) or by 1.7.1.

In the remaining case ($p\nmid n$, or $p|n$, $a_{n-1} \neq 0$), we apply the same lemmas 1.6.3.1, 1.7.1 and 1.7.3 to ensure that one and only one place of K at finite distance of (5) is singular.

The foregoing process can be improved significantly if better criteria of k-smoothability were available, especially when $c \notin k_s$.

2. Hyperelliptic forms of the affine line

In this section, k is assumed to be separably closed ($k = k_s$).

2.0. In KMT - §6 we have described all k-forms of A^1 of arithmetic genera ≤ 1 carrying a k-rational point; cf. KMT - 6.8.1, 6.8.3, and also Russell [17], Queen [10]. We now proceed to describe all hyperelliptic curves that are k-forms of A^1, assuming $k = k_s$. As a by-product, we obtain a complete description of all k-forms of A^1 of arithmetic genus 2 carrying a k-rational point.

2.1.1. LEMMA. *Every hyperelliptic k-curve of genus $g \geq 2$ is k-birationally equivalent to an affine plane curve of either type:*

(i) (if $p > 2$) $y^2 = f(x) \in k[x]$; $\deg f = 2g + 1$ or $2g + 2$;

(ii) (if $p = 2$) $y^2 + f(x)y + h(x) = 0$; $f(x) \in k[x]$, $\deg f \leq g + 1$; $h(x) \in k[x]$, $\deg h = 2g + 2$;

such that in both cases (i), (ii) the point at infinity of the plane curve is k-smoothable.

It is of course well-known that the equations of the above type represent k-birationally all hyperelliptic k-curves of a given genus g (cf. [1; XVI, §7]). The point of our lemma is the realizability of the last provision concerning the point at infinity.

Proof. Let $K = k(x,y)$ be the function field, and $k[x,y]$ the coordinate ring of the affine curve (i) or (ii). Let o be a place of K, *at infinity* of the curve in question. This is so if and only if $k[x,y] \not\subseteq o$,

which is equivalent to $x \notin o$ because y is integral over $k[x]$. Now observe that if each place at infinity (there may be several such) is smooth then the point at infinity is k-smoothable, and vice versa. Now, in either case (i) or (ii), after suitable change of coordinates $(x,y) \longmapsto (x - a, y)$, $a \in k$, we may assume that the points, $(x = 0, y = \pm\sqrt{f(0)})$ in case (i) and $(x = 0, y =$ roots of $Y^2 + f(0)Y + h(0) = 0)$ in case (ii), are all smooth (noting k is infinite). Let o_1, o_2 be the smooth places corresponding to these points. (Possibly $o_1 = o_2$, but no matter.) Consider the following k-birational substitutions:

$$x = 1/\xi,\ y = \eta/\xi^{g+1},\ \text{so}\ \ k(x,y) = k(\xi, \eta).$$

Then, one easily verifies the equations

$$\text{(i')} \quad \eta^2 = \xi^{2g+2} f(1/\xi) = \phi(\xi) \in k[x],\ \deg\phi = 2g + 1 \ \text{ or } \ 2g + 2\ ;$$

$$\text{(ii')} \quad \eta^2 + \xi^{g+1} f(1/\xi)\eta + \xi^{2g+2} h(1/\xi) = \eta^2 + \phi(\xi)\eta + \psi(\xi) = 0\ ;$$

$$\phi(x) \in k[x],\ \deg\phi \le g + 1\ ;\ \psi(x) \in k[x],\ \deg\psi = 2g + 2\ ,$$

corresponding to (i), (ii), respectively. Since x belongs to the maximal ideals of o_1, o_2 and $x = 1/\xi$, the places o_1, o_2 are at infinity of the (ξ, η)-curves (i'), (ii'), and clearly these are the only ones at infinity. Thus, we have shown that in the new form (i') or (ii') according as $p > 2$ or $p = 2$, our k-curve is k-smoothable at infinity. Q.E.D.

2.1.2. LEMMA. *Let C be a hyperelliptic affine plane k-curve of genus $g \ge 2$, defined by an equation of either type (i) or (ii) of 2.1.1 and having a k-smoothable point at infinity. Then, C is k-normal.*

Proof. Firstly, the case $p > 2$ with eqn. (i): By standard homogenization followed by a suitable dehomogenization, the point at infinity may be identified as $(t = 0, u = 0)$ of the plane curve

$$t^{n-2} = u^n + a_1 u^{n-1} t + \ldots + a_{n-1} u t^{n-1} + a_n t^n$$

with multiplicity $n - 2$, where we have put $n = 2g + 1$ or $2g + 2$. The blowing-up of this curve at $(t = 0, u = 0)$ is effected by putting $v := t/u$, and one gets

$$v^{n-2} = u^2(1 + a_1 v + \ldots + a_n v^n)$$

as a local equation for the proper transform. It is easy to see that the point $(u = 0, v = 0)$ of multiplicity 2 is the only point lying over $(t = 0, u = 0)$. Now perform blowing-up of $(u = 0, v = 0)$ $g - 1$ times in succession. This operation amounts to introducing variables $u_1, \ldots, u_{g-1}$ by $u = vu_1$, $u_1 = vu_2$, $\ldots$, $u_{g-2} = vu_{g-1}$. At each stage one gets a unique singular point of multiplicity 2, until one ends up with equations

$$v = u_{g-1}^2(1 + a_1 v + \ldots + a_n v^n) \quad \text{if} \quad n = 2g + 1,$$
$$v^2 = u_{g-1}^2(1 + a_1 v + \ldots + a_n v^n) \quad \text{if} \quad n = 2g + 2.$$

The point $(u_{g-1} = 0, v = 0)$ is in either case the unique point lying over the original $(t = 0, u = 0)$; it is smooth in the first case of $n = 2g + 1$, and is an ordinary double point in the remaining case. This double point is resolved into two smooth points by one more blowing-up $u_{g-1} = vu_g$, as one easily ascertains. Consequently, by virtue of 0.2.1 and 0.2.3, the arithmetic k-genus of the proper transform after the foregoing series of blowing-ups is

$(n - 1)(n - 2)/2 - (n - 2)(n - 3)/2 - \alpha$ where $\alpha = g - 1$ if $n = 2g + 1$ and $\alpha = g$ if $n = 2g + 2$. The said arithmetic genus is thus equal to $n - 2 - \alpha = g$ in either case. Since C is assumed to have k-genus g, C cannot have any non-k-normal point in view of 0.2.2 and the remark following it.

Next, the case $p = 2$ with eqn. (ii): Since the calculations are very similar to the preceding case, we shall merely outline the steps to be taken, as follows. Homogenize and then dehomogenize eqn. (ii) so as to bring the original point at infinity down to the origin, which turns out to have multiplicity $2g$ on the curve. Blow it up to get a unique point lying over the origin, with multiplicity 2. One continues to blow up in succession, altogether g times, and the resulting sequence of multiplicities is $(2g, 2, \ldots, 2)$. At this last stage, a local equation for the singular point $(u = 0, v = 0)$ may be written as

$$u^2 + (a_d + a_{d-1}u + \ldots + a_0u^d)u^{g+2-d}v$$

$$+ (b_{2g+2} + b_{2g+1}u + \ldots + b_0u^{2g+2})v^2 = 0$$

where $f(x) = \sum_1^d a_i x^i$ with $d \leq g + 1$, $a_d \neq 0$ and $h(x) = \sum_1^{2g+2} b_j x^j$ in reference to equation (ii) of 2.1.1. Blow up $(u = 0, v = 0)$ once more, and one gets either two smooth points or one possibly singular point according as $d = g + 1$ or $d < g + 1$. Through $g + 1$ blowing-ups thus far, the arithmetic genus has dropped down to

$$(2g + 2 - 1)(2g + 2 - 2)/2 - 2g(2g - 1)/2 - g = g.$$

Therefore, the latest proper transform just now be k-normal, which implies the k-normality of C.

2.1.2. Remark. We have actually shown above that, in case $p > 2$, the point at infinity of a k-curve defined by (i) is always k-smoothable. We can prove that, when $p = 2$, the curve given by (ii) is k-smoothable at infinity except in the case: $d < g$, $b_{2g+2} \notin k^2$ and $b_{2g+1} = 0$ in the notations of the preceding proof. We shall not be needing these results, though.

2.2. THEOREM. Let K be a separably closed nonperfect field of characteristic $p > 2$. Then, a hyperelliptic k-form of A^1, of k-genus $g \geq 2$, is k-birationally equivalent to an affine plane k-curve of the type

$$y^2 = x^{p(m)} - a, \text{ where } a \in k - k^p,$$

with $g = (p^m - 1)/2$. Conversely, the complete k-normal model C of every such plane curve has a unique singularity P, and $C - \{P\}$ is a k-form of A^1 of k-genus $(p^m - 1)/2$.

Proof of this result will be given in the following paragraphs:

2.2.1. Let C be a hyperelliptic k-curve of genus g defined by an equation $y^2 = f(x)$ as in 2.1.1 (i), the point at infinity being k-smoothable. Remembering $k = k_s$, decompose $f(x)$ into a product of irreducible factors over k:

$$f(x) = \prod_i P_i(x)^{\nu(i)} \times \prod_j Q_j(x)^{\mu(j)}$$

with distinct $P_i(x)$'s of type $x^{p(m)} - a$ ($m > 0$, $a \in k - k^p$) and distinct $Q_j(x)$'s of type $x - b$ ($b \in k$). Note that one may actually assume all exponents $\nu(i) = \mu(j) = 1$. Indeed, if $f(x) = g(x)^{2r+s}h(x)$ with $g(x)$

irreducible, $\gcd(g(x), h(x)) = 1$ and $s = 0$ or 1, then by the birational change of variables $x' = x$, $y' = y/g(x)^r$ the equation $y^2 = f(x)$ is transformed into $y'^2 = g(x')^s h(x')$ and the places at infinity of the new plane curve are exactly the same as those at infinity of the old curve. Therefore let anew

$$y^2 = f(x) = P_1(x) \ldots P_t(x)Q_1(x) \ldots Q_u(x) \tag{1}$$

be the decomposition as above with distinct irreducible factors $P_i(x)$'s and $Q_j(x)$'s. Assume, now, that C is k-birationally equivalent to a k-form of $\mathbb{A}^1$. This assumption is equivalent to (a) the function field $K := k(x,y)$ of C has exactly one singular place, and (b) the $\bar{k}$-genus of K is zero (cf. 0.2). The consequences of (a) and (b) will now be deduced.

2.2.2. As the places at infinity of the curve defined by (1) are all smooth by 2.1.1, there must be exactly one singular place at finite distance of the curve (1) in view of (a) above. This entails $t = 1$ in (1). For, if $P(x) = x^{p(m)} - a$ is any one of the $P_i(x)$'s, then $(x = a^{p(-m)}, y = 0)$ is a singular point as seen by Jacobian criterion, but its local ring has a principal maximal ideal (y) and is therefore a valuation ring; thus each $P_i(x)$ gives out a singular place, so only one such factor is present. Thus,

$$y^2 = (x^{p(m)} - a)(x - b_1) \ldots (x - b_s) \tag{2}$$

is our equation.

2.2.3. Let us now extend the scalar field k to the algebraic closure $\bar{k}$, and regard (2) as a defining equation of a $\bar{k}$-curve. The $\bar{k}$-rational point

$(x = a^{p(-m)},\ y = 0)$ is not $\overline{k}$-normal and has multiplicity 2. One performs $\overline{k}$-normalization through a series of blowing-ups beginning with substitution $y := wt,\ w := x - a^{p(-m)}$. After each blowing-up one obtains either a non-$\overline{k}$-normal point of multiplicity 2 or a $\overline{k}$-normal point. In the former case, blow it up. Each blowing-up here causes a genus drop of $\frac{2(2-1)}{2} = 1$ (cf. 0.2.1). After $(p^m - 1)/2$ times blowing-ups, one is led to an equation of the type

$$T^2 = W(W - \beta_1) \ldots (W - \beta_s)$$

with nonzero and mutually distinct $\beta_1, \ldots, \beta_s \in \overline{k}$, which clearly represents a $\overline{k}$-smooth affine curve. In this process of blowing-ups over $\overline{k}$ the arithmetic genus drops by $(p^m - 1)/2$ which is the number of blowing-ups conducted. In view of (b), we then have $g = (p^m - 1)/2$. On the other hand, the degree of $(2) = p^m + s = 2g + 1$ or $= 2g + 2$, whence follows $s = 0$ or 1. However, the case $s = 1$ is easily reduced to the other case of $s = 0$. Indeed: If $y^2 = (x^{p(m)} - a)(x - b)$, then, as one may assume $b = 0$ by replacing x by $x - b$ and a by $a - b^{p(m)}$, one can view it as

$$y^2/x^{p(m)+1} = (1 - a/x^{p(m)}).$$

Therefore, through the birational transformation $(x,y) \longmapsto (z = 1/x,\ w = y/x^{(p(m)+1)/2})$ one obtains

$$w^2 = (1 - az^{p(m)})$$

which is equivalent to an equation of type (2) with $s = 0$. All in all, our function field is identifiable with that of an affine plane k-curve of the

type

$$y^2 = x^{p(m)} - a \; ; \quad a \in k - k^p \tag{3}$$

with genus $g = (p^m - 1)/2$.

2.2.4. From the foregoing analysis it is obvious, conversely, that the k-normal completion of the affine curve (3), after its unique singularity is removed, gives an affine k-curve of genus $g = (p^m - 1)/2$ which is a k-form of A^1. This completes the proof of 2.2.

2.3. THEOREM. Let k be a separably closed nonperfect field of characteristic 2. Then a hyperelliptic k-form of A^1, of k-genus $g \geq 2$, is k-birationally equivalent to an affine plane k-curve of one of the following types:

(A) $y^2 + (x^{2(i)} + a)^{2(\ell)} y + b = 0$, where $i \geq 0$, $\ell \geq 0$, $a \in k$, $b \in k - \{0\}$; $a \notin k^2$ if $i > 0$, $b \notin k^2$ if $\ell > 0$; and $g = 2^{i+\ell} - 1$.

(B) $y^2 = x(x + \alpha)^{2g} + E(x)$, where $\alpha \in \overline{k}$, $(x + \alpha)^{2g} \in k[x]$, $E(x) \in k[x]$ is an even polynomial of degree $2g + 2$, and $E(\alpha) \notin k^2$ in case $\alpha \in k$.

Conversely, the k-normal completion of every curve of either type (A) or type (B), minus its unique singularity, is a k-form of A^1; of k-genus = g in case (A), of k-genus $\leq g$ in case (B).

The proof of the theorem will be given in the rest of this section (§2).

2.3.1. Let C be a hyperelliptic k-curve of genus g defined by an equation

$$y^2 + f(x)y + h(x) = 0 \tag{4}$$

subject to the conditions enunciated in 2.1.1 (ii). Assume that C is k-birationally equivalent to a k-form of A^1. Just as before, this is equivalent to assuming the two conditions (a) and (b) of 2.2.1 concerning the function field $K = k(x,y)$ of C. Then C is k-normal by 2.1.2 and smooth except at precisely one point, the point at infinity being k-smoothable by 2.1.1.

2.3.1.1. PROPOSITION. *With the foregoing notations and assumptions, the coefficient* $f(x)$ *of* y *in* (4) *is either* 0 *or* $c(x + \alpha)^{g+1}$, *where* $c \in k - \{0\}$ *and* $\alpha \in \bar{k}$.

Proof. Suppose that $f(x) \neq 0$ and call $S = (x = \alpha, y = \beta)$ the unique k-normal singular point on C which is a one-place point. S is clearly not k-rational. From the Jacobian criterion used over $\bar{k}$ follows that the elements α, β of $\bar{k}$ must satisfy

$$f(\alpha) = 0,\ f'(\alpha)\beta + h'(\alpha) = 0 \quad \text{and} \quad \beta^2 + h(\alpha) = 0. \tag{5}$$

If $\alpha \in k$, then $f'(\alpha) = 0$, for otherwise $\beta = f'(\alpha)^{-1}h'(\alpha) \in k$ and S would be k-rational. If $\alpha \notin k$, then $f(x) = (x^{2(i)} + a)f_1(x)$ for some $f_1(x) \in k[x]$, $\alpha^{2(i)} = a$ with $i > 0$, and $f'(\alpha) = 0$ again. In either case,

$$f(x) = (x + \alpha)^m f_1(x) \tag{6}$$

with $2 \leq m \leq g + 1$, where $f_1(x) \in k[x]$ and $f_1(\alpha) \neq 0$. By putting $X := x + \alpha$, $Y := y + \beta$, one can rewrite (4) as

$$\overline{C} : Y^2 + X^m f_1(X + \alpha)Y + h_1(X) = 0 \tag{7}$$

where $h_1(X) = f(X + \alpha)\beta + \beta^2 + h(X + \alpha)$, and $h_1(0) = 0$ as a consequence of (5). Since the $\overline{k}$-curve C must have the point $(X = 0, Y = 0)$ as a singularity of multiplicity $(2, 2, \ldots, 2, 1, 1, \ldots)$ becoming $\overline{k}$-smooth only after g blowing-ups, one can deduce that $m = g + 1$ by virtue of Lemma 2.3.1.2 below. Therefore, from (6) follows $f(x) = c(x + \alpha)^{g+1}$.

2.3.1.2. LEMMA. Let $\overline{B}$ be the affine $\overline{k}$-curve defined by

$$\overline{B} : Y^2 + X^n F(X)Y + (b_0 + b_1 X + \ldots + b_m X^m) = 0 \tag{8}$$

where $n > 1$, $F(X) \in \overline{k}[x]$, $F(0) \neq 0$, $H(X) := b_0 + b_1 X + \ldots + b_m X^m \in \overline{k}[X]$. Then, the point $(X = 0, Y = b_0^{1/2})$ on $\overline{B}$ is a singularity of multiplicity 2 if and only if $b_1 = 0$. Moreover, when that is so, one blowing-up centered at $(X = 0, Y = b_0^{1/2})$ transforms $\overline{B}$ into

$$\overline{B} : Y^2 + X^{n-1}F(X)Y + b_0^{1/2}X^{n-2}F(X) + b_2 + b_3 X + \ldots + b_m X^{m-2} = 0. \tag{9}$$

Proof. The first assertion is an immediate consequence of the Jacobian criterion. Suppose now $b_1 = 0$. Then, putting $Z := Y - b_0^{1/2}$, we rewrite (8) as

$$Z^2 + X^n F(X)Z + b_0^{1/2}X^n F(X) + (b_2 X^2 + \ldots + b_m X^m) = 0.$$

Then, the blowing-up centered at $(X = 0, Z = 0)$ is effected by putting $Z = XY_1$, and we get

$$Y_1^2 + X^{n-1}F(X)Y_1 + b_0^{1/2}X^{n-2}F(X) + (b_2 + \ldots + b_m X^{m-2}) = 0,$$

which is as asserted.

2.3.2. We shall now assume the affine plane k-curve C defined by

$$C : y^2 + c(x + \alpha)^{g+1}y + h(x) = 0, \; c \neq 0 \tag{10}$$

to be k-birationally equivalent to a k-form of A^1 of k-genus g, subject to the restriction that the unique singular place is at finite distance from C. By dividing (10) through by c^2 and rewriting y/c as y, we may assume c = 1.

2.3.2.1. Observe first that through a series of k-automorphisms of the (x,y)-plane, the equation (10) for C (with c = 1) can be transformed into one for which deg h(x) $\leq$ g. Indeed, when $h(x) = bx^{2g+2}$ + (terms of lower degree), the term bx^{2g+2} is eradicated through the substitution $(x,y) \longmapsto (x, y + ax^{g+1})$ where $a \in k$ satisfying $a^2 + a + b = 0$. Next, when $h(x) = bx^d$ + (terms of lower degree) and $g + 1 \leq d < 2g + 2$, then substitute $y + bx^{d-g-1}$ for y; then $(y + bx^{d-g-1})^2 = y^2 + b^2x^{2(d-g-1)}$, $(x + \alpha)^{g+1}(y + bx^{d-g-1}) = (x + \alpha)^{g+1}y + bx^d$ + (polynomial in x of degree < d) and $d - 2(d - g - 1) = 2g + 2 - d > 0$, so that the leading term bx^d of h(x) has been eliminated. In this and the subsequent paragraphs through 2.3.2.4, we shall deviate from the assumption of 2.3.1 and assume, as we may, that deg h(x) $\leq$ g in (10).

2.3.2.2. Next we claim that, under our assumptions of 2.3.2 - 2.3.2.1, the polynomial h(x) is even. To see this, write Y = y, X = x + α in (10) to obtain

$$B : Y^2 + X^{g+1}Y + H(X) = 0 \qquad (11)$$

where we have put $H(X) := h(X + \alpha) = \beta_0 + \beta_1 X + \ldots + \beta_g X^g \in \overline{k}[X]$. We now apply 2.3.1.2 repeatedly: (i) In case $g + 1 = 2r$, blow up the unique singularities of B and of its proper transforms r times in succession, which is possible because $g - r = r - 1 > 0$ as $g \geq 2$. The resulting equation over $\overline{k}$ is

$$Y^2 + X^{g+1-r}Y + \beta_0^{1/2} + \beta_2^{1/2}X + \ldots + \beta_{g-1}^{1/2}X^{g-r} = 0$$

with $\beta_1 = \beta_3 = \ldots = \beta_g = 0$. (ii) In case $g = 2r$, repeat the same process r times to get

$$Y^2 + X^{g+1-r}Y + \beta_g + \beta_0^{1/2}X + \ldots + \beta_{g-2}^{1/2}X^{g-r} = 0$$

with $\beta_1 = \beta_3 = \ldots = \beta_{g-1} = 0$. In both cases, therefore, $H(X)$ is an even polynomial. Now, if $h(x)$ contained any terms of odd degree, look at the one of the highest odd degree; it would certainly contribute a term of odd degree in $h(X + \alpha) = H(X)$, contrary to the result obtained just now. Our claim is now justified.

2.3.2.3. One can push the arguments of the preceding paragraph further: After $r = [(g + 1)/2]$ blowing-ups the coefficient of Y in our equation is X^{g+1-r}; if $g + 1 - r > 1$, then perform $[(g + 1 - r)/2]$ successive blowing-ups which will allow us to deduce that $\beta_{2i} = 0$ for all odd i in case $g + 1 - r$ is even, and that $\beta_{2j} = 0$ for all even j in case $g + 1 - r$ is odd. This process continues until the second term of our equation is XY, and altogether g blowing-ups have been performed. Consequently, all but one

β_i are zero, and i is even in view of 2.3.2.2. This means that $h(X + \alpha) = H(X) = \beta_{2m}X^{2m}$, a monomial of even degree $2m \geq 0$, hence $h(x) = \beta_{2m}(x + \alpha)^{2m}$.

2.3.2.4. We have reached a point where the initial equation (10) has been simplified to

$$C_0 : y^2 + (x + \alpha)^{g+1}y + b(x + \alpha)^{2m} = 0 \qquad (12)$$

where $0 \leq 2m \leq g$, $b \in k$, and $(x + \alpha)^{g+1}$, $(x + \alpha)^{2m}$ both belong to $k[x]$. Note that the reduction from C by (10) to C_0 above has been made through the k-automorphisms of the (x,y)-plane of type $(x,y) \longmapsto (x, sy + P(x))$ with $s \in k - \{0\}$, $P(x) \in k[x]$ only. It is therefore clear that the affine curves C, C_0 are k-isomorphic and the unique place at infinity of C correspond k-isomorphically with the one at infinity of C_0. More precisely, we have

2.3.2.5. LEMMA. *A plane k-curve defined by*

$$y^2 + f(x)y + h(x) = 0$$

satisfying $\deg f = g + 1$, $\deg h \leq g$ *has a unique one-place point* P *at infinity, of multiplicity* g. *The point* P_1 *infinitely near* P *in the first neighborhood is smooth. The genus of the curve is* $\leq g$, *the equality holding if and only if the curve is k-normal*

We omit the proof of this lemma, as it is an easy exercise in blowing-up.

2.3.3. We shall now return to the consideration of C_0 above, dividing the cases into two:

Case 1: $\alpha \in k$. Then, C_0 is clearly k-isomorphic to C_1 given by

$y^2 + x^{g+1}y + bx^{2m} = 0$. If $m > 0$, this would in turn be k-birationally equivalent to

$$C_1' : z^2 + x^{g+1-m}z + b = 0$$

through the substitution $z = y/x^m$, so that by Lemma 2.3.2.5 above the k-genus of $k(C_1') = k(C_0)$ is no more than $g - m$, an absurdity. Hence $m = 0$ must hold. So, in this case, our equation (12) for C_0 has been brought down to

$$y^2 + x^{g+1}y + b = 0$$

which is a special case of (A)-type curves in 2.3. We have proved

2.3.3.1. PROPOSITION. (a) The notations and assumptions being the same as in 2.3.2, assume that the unique singular place of $k(C)$ induces a k-rational place on $k(x)$, the unique rational subfield of $k(C)$. Then, through k-automorphism of the (x,y)-plane, C is k-isomorphic to a plane k-curve.

$$C_1 : y^2 + x^{g+1}y + b = 0 \qquad (13)$$

with $b \in k - k^2$, $g = 2^\ell - 1$ with $\ell \geq 2$.

(b) Conversely, such C_1 is k-birationally equivalent to a k-form of A^1 of k-genus g, whose unique singular place is k-rational when restricted to the unique rational subfield $k(x)$.

2.3.3. (resumed). Case 2: $\alpha \notin k$. Then $\alpha^{2(i)} = a \in k$, $\alpha^{2(i-1)} \notin k$ for some $i > 0$. As $(x + \alpha)^{g+1} \in k[x]$ in (12), $g + 1$ must be even. Put $u := x^2$ and rewrite (12) as follows:

$$C_0^{(1)} : y^2 + (u + \alpha^2)^{(g+1)/2} y + b(u + \alpha^2)^m = 0. \qquad (14)$$

There is a natural finite k-morphism $C_0 \longrightarrow C_0^{(1)}$ arising from the inclusion $k[u,y] \hookrightarrow k[x,y]$. The only possible singular point of $C_0^{(1)}$ is $(u = \alpha^2 \; ; \; y = 0$ if $m > 0$, $y = b^{1/2}$ if $m = 0)$ which is dominated by the unique singular point of C_0. Denote by $o^{(1)}$ and o the local rings at these respective points. Then clearly $o = o^{(1)}[x]$ and o is a faithfully flat extension of $o^{(1)}$ of rank 2. Because o is k-normal by assumption, $o^{(1)}$ is k-normal, too. Thus $C_0^{(1)}$ is everywhere k-normal, whence $k(C_0^{(1)})$ is of genus exactly $(g + 1)/2 - 1 = (g - 1)/2$ in consideration of 2.3.2.5. The field $k(C_0^{(1)})$ is contained in $k(C_0)$ which is a k-form of the rational function field $k(t)$. Hence $k(C_0^{(1)})$ itself is a k-form of $k(t^2)$ by Lüroth's Theorem. The possible singularity mentioned above on $C_0^{(1)}$ is a one-place singularity because the corresponding singularity on C_0 is such. We conclude, therefore, that $C_0^{(1)}$ is a (possibly trivial) k-form of A^1 of k-genus $(g - 1)/2$. This entails further the following: If $\alpha^2 \in k$ or $i = 1$, then $m = 0$, $(g - 1)/2 = 2^{\ell} - 1$ with $\ell \geq 1$, and $b \in k - k^2$, by the results of Case 1. Then $g = 2^{\ell+1} - 1$. If on the other hand $\alpha^2 \notin k$ or $i > 1$, then m is even by 2.3.2.3, and $(g + 1)/2$ is clearly even, too. Thus one can make another substitution $w := u^2$ in (14) to get $C_0^{(2)}$, a k-form of A^1 of k-genus $[(g - 1)/2 - 1]/2$. And so on. In this fashion, one can reach

$$C_0^{(i)} : y^2 + (u + a)^N y + b(u + a)^M = 0,$$

where $N = (g + 1)/2^i$, $M = m/2^{i-1}$, $M < N$, and $C_0^{(i)}$ is a (possibly trivial) k-form of A^1 of k-genus $N - 1$. If $N - 1 \geq 2$, then $M = 0$ and $N - 1 = 2^{\ell} - 1$, $\ell \geq 2$ by Case 1. If $N - 1 = 1$ (hence $M \leq 1$), $C_0^{(i)}$ has a unique singular point determined by $u = a$. Hence $M = 0$. If

$N - 1 = 0$, $M = 0$ since $M < N$. In any case, we have $M = 0$ (whence $m = 0$), and $N - 1 = 2^{\ell} - 1$, $\ell \geq 0$. Thus $g = 2^{i+\ell} - 1$, $i > 0$, $\ell \geq 0$, $i + \ell \geq 2$. Unless $N = 1$, $b \in k - k^2$ is required for $C_0^{(i)}$ to have genus $N - 1$.

We formulate the results thus far as a proposition, whose converse part should be obvious from the foregoing discussion:

2.3.3.2. PROPOSITION. (a) The notations and assumptions being the same as in 2.3.2, assume that the unique singular place of $k(C)$ induces a non- k-rational place on $k(x)$. Then, through k-automorphism of the (x,y)-plane, C is k-isomorphic to a plane k-curve

$$C_2 : y^2 + (x^{2(i)} + a)^{2(\ell)}y + b = 0 \tag{15}$$

where $i > 0$, $\ell \geq 0$, $i + \ell \geq 2$, $a \in k - k^2$, $b \in k - \{0\}$, and $b \notin k^2$ if $\ell > 0$; and the relation $g = 2^{i+\ell} - 1$ gives the k-genus.

(b) Conversely, such C_2 is k-birationally equivalent to a k-form of A^1 of k-genus $g = 2^{i+\ell} - 1$, whose unique singular place is non- k-rational when restricted to the unique rational subfield $k(x)$.

2.3.4. We shall now turn back to the situation preceding 2.3.2 and shall deal with the remaining case of $f(x) = 0$ (absent) in equation (4) (cf. 2.3.1.1).

2.3.4.1. PROPOSITION. Assume that the point at infinity of the curve

$$B : y^2 = h(x) = b_0 + b_1x + \ldots + b_{2g+2}x^{2g+2} \quad (b_{2g+2} \neq 0) \tag{16}$$

is either smooth or smoothable over k (cf. 2.1.1). Write

$h(x) = E_1(x) + E_2(x)x$ *with* E_1, E_2 *even polynomials in* $k[x]$. *Then:*

(a) *If* $k(B)$ *is a function field of a* k*-form of* A^1 *of* k*-genus* g, *then*

$$E_2(x) = b(x + \alpha)^{2g} \tag{17}$$

with $b \in k$, $b \neq 0$, $\alpha \in \bar{k}$, *and* $E_1(\alpha) \notin k^2$ *if* $\alpha \in k$.

(b) *Conversely, if* $E_2(x)$ *is as in* (17) *satisfying the accompanying conditions, then* $k(B)$ *is a function field of a* k*-form of* A^1 *of* k*-genus* $\leq g$.

Proof. (a) If B is k-birationally equivalent to a k-form of A^1, then by 2.1.2 B has precisely one k-normal non- k-rational singular point S and all other points of B must be smooth. Thus, if $S = (x = \alpha, y = \beta)$, then $\beta^2 = E_1(\alpha)$, $E_2(\alpha) = 0$, and (α,β) is the unique pair in $\bar{k} \times \bar{k}$ satisfying these two relations. It follows from this and from 1.7.4 that E_2 is in the form of (17). Moreover, since S is non- k-rational, either $\alpha \notin k$ or $E_1(\alpha) \notin k^2$.

(b) Conversely, suppose that $h(x) = E_1(x) + E_2(x)x$ satisfies the stated conditions. Then, by 1.5.1, $k(B)$ is a k-form of $k(t)$ and its k-normal completion C has exactly one one-place singularity S at finite distance on B. Therefore, $C - S$ is a k-form of A^1. The genus drop effected by S brings down the k-genus to no more than g.

2.3.4.2. *Remark.* Given B as in 2.3.4.1 (b), one does not possess at one's disposal means to decide whether or not $S = (x = \alpha, y = \beta)$ is k-normal. If it is not, the arithmetic genus of C becomes less than g. In general, one

can only say that the genus of C is $\leq g$.

Conclusion of Proof: The foregoing paragraphs, in particular Propositions 2.3.3.1 - 2 and 2.3.4.1, clearly establish the truth of our Theorem 2.3.

2.4. We now proceed to determine all k-forms of A^1 of k-genus 2. Such a k-form must be hyperelliptic, for if otherwise the canonical series would define a k-birational morphism of the k-form into $P_k^{2-1} = P_k^1$ (cf. Chevalley [2; VI, §9, Th. 10]). Thus, as an immediate consequence of Theorems 2.2 and 2.3, we have

THEOREM. The k-forms of A^1 of genus 2 exist only if the characteristic p of the separably closed ground field k is either 2 or 5. Such a k-form is k-birationally equivalent to one of the following k-normal affine plane curves:

(I) In case $p = 2$:

$$C : y^2 = x(x + \alpha)^4 + E(x)$$

where $\alpha^4 \in k$, $E(x) \in k[x]$ is even of degree 6, and either $\alpha \notin k$ or $E(\alpha) \notin k^2$.

(II) In case $p = 5$:

$$D : y^2 = x^5 + a, \quad a \in k - k^5.$$

3. Automorphisms of the forms of the affine line.

3.0. Let X be a nontrivial k-form of A^1. In KMT - 6.9.1, we saw following Russell that in case $k = k_s$ the group $\mathrm{Aut}_k(X)$ of biregular k-automorphisms of X is an infinite group if and only if $X = \overline{G}$ for some k-group of Russell type. (As in KMT, we denote by $\overline{G}$ the underlying scheme of a group scheme G.) We saw also that a k-form of A^1, birationally equivalent to an affine plane curve $y^2 = x^5 - a$, where $p = 5$ and $a \in k - k^5$, has exactly two biregular k-automorphisms (cf. KMT - 6.9.3). In this section, we shall show among other things that if $p > 2$ every hyperelliptic k-form of A^1 has exactly two biregular k-automorphisms, and shall construct a k-form of A^1 with m biregular k-automorphisms for each characteristic $p > 2$ and a positive integer m such that $(p,m) = (p, m + 1) = 1$.

3.1. Let X be a nontrivial k-form of A^1, A the affine k-algebra of X, and $K = k(X)$ the function field of X over k. Let C be the k-normal completion of X, and let $P_\infty := C - X$. We denote by $\mathrm{Aut}_k(X)$ the group of all biregular k-automorphisms of X, and by $\mathrm{Aut}_k(C)$ the group of all biregular k-automorphisms of C. Since C is k-normal, $\mathrm{Aut}_k(C)$ coincides with the group of all birational k-automorphisms of K.

3.1.1. PROPOSITION. *With the notations and assumptions as above:*

(i) *If the height* $\mathrm{ht}(K)$ *of* K *is positive,* $\mathrm{Aut}_k(X) = \mathrm{Aut}_k(C)$.

(ii) *If* $\mathrm{ht}(K)$ *is zero and* X *is non-isomorphic to the affine plane curve* $y^2 = x + ax^2$, *where* $p = 2$ *and* $a \in k - k^2$, *then* $\mathrm{Aut}_k(X) = \{1\}$.

Proof. (i) If $ht(K) > 0$ then P_∞ is a unique k-normal singular point of C. Therefore every element σ of $Aut_k(C)$ fixes the point P_∞. Thus σ induces a biregular k-automorphism $\sigma|_X$ of $Aut_k(X)$. Conversely, each element τ of $Aut_k(X)$ is extendable to an element $\tilde{\tau}$ of $Aut_k(C)$ since C is k-normal. It is obvious that $\widetilde{(\sigma|_X)} = \sigma$ and $\tilde{\tau}|_X = \tau$. Therefore the correspondences $\sigma \longmapsto \sigma|_X$ and $\tau \longmapsto \tilde{\tau}$ establish an isomorphism between $Aut_k(X)$ and $Aut_k(C)$.

(ii) If $ht(K) = 0$, then C is isomorphic to P^1_k, and P_∞ is a non- k-rational point of C. Choose an inhomogeneous parameter t of P^1_k such that $t^{p(n)} = a$ at P_∞ with $a \in k$ and $a \notin k^p$. Take an element σ of $Aut_k(X)$. Then σ, extended to an element of $Aut_k(C)$, fixes P_∞. Write $\sigma(t) = (bt + c)/dt + e)$ with b, c, d, e $\in$ k, and $\alpha^{p(n)} = a$ with $\alpha \in k^{p(-n)}$. Then we have; $d\alpha^2 + (e - b)\alpha - c = 0$. Since X is not isomorphic to $y^2 = x + ax^2$ with $p = 2$ and $a \in k - k^2$, either $p \neq 2$, or $p = 2$ and $n \geq 2$. Then 1, α and α^2 are linearly independent over k. Hence $d = c = 0$ and $e = b$, i.e., $\sigma(t) = t$. Namely σ is the identity. (Needless to say, if $p = 2$ and $n = 1$, X is isomorphic to the plane curve $y^2 = x + ax^2$.) Q.E.D.

3.1.2. COROLLARY. Assume that $ht(X) > ht(K)$, and that either $p > 2$ or $ht(X) - ht(K) \geq 2$. Then $Aut_k(X) = \{1\}$.

Proof. There exists a purely inseparable algebraic extension k' of k such that $X \otimes k'$ is k'-rational but is not k'-isomorphic to $A^1_{k'}$. Further, if $p = 2$ then we may assume $ht(X \otimes k') \geq 2$. It is clear that $Aut_k(X)$ is a subgroup of $Aut_{k'}(X \otimes k')$; but part (ii) of 3.1.1 implies that

$\mathrm{Aut}_{k'}(X \otimes k') = \{1\}$. Therefore $\mathrm{Aut}_k(X) = \{1\}$. Q.E.D.

3.1.3. COROLLARY. Let G be a k-group of Russell type (cf. KMT - 2.7). Then, $\mathrm{ht}(\overline{G}) = \mathrm{ht}(k(\overline{G}))$ if $p > 2$, and $\mathrm{ht}(\overline{G}) - \mathrm{ht}(k(\overline{G})) \leq 1$ if $p = 2$.

This is clear from 3.1.2 and from the fact that $\mathrm{Aut}_{k_s}(\overline{G} \otimes k_s)$ is infinite.

3.1.4. Examples. (i) Let G be a Russell-type k-group $y^{2(n)} = x + ax^2$ with $p = 2$, $n \geq 1$ and $a \in k - k^2$. Then $\mathrm{ht}(\overline{G}) = n$ and $\mathrm{ht}(k(\overline{G})) = n - 1$.

(ii) Let G be a Russell-type k-group $y^{2(n)} = x + ax^4$ with $p = 2$, $n \geq 1$, and $a \in k - k^2$. Then $\mathrm{ht}(\overline{G}) = n$ and $\mathrm{ht}(k(\overline{G})) = n$.

3.1.5. THEOREM. For each k-form X of A^1, there is a canonical finite purely inseparable morphism $X \longrightarrow A^1$, causing an injective homomorphism

$$\mathrm{Aut}_k(X) \longrightarrow \mathrm{Aut}_k(A^1).$$

Proof. Write $X = \mathrm{Spec}\ A$ and call $\lambda = \mathrm{ht}(X)$. Then, by 1.5.2 (b), $k[A^{p(\lambda)}] = k[u]$ for some $u \in A$, and $X \longrightarrow A^1$ arising from the inclusion $k[u] \hookrightarrow A$ is the desired canonical morphism. Since every automorphism of A must send $k[u]$ onto itself because of the latter's invariantive nature, and since $A^{p(\lambda)} \subseteq k[u]$, the group $\mathrm{Aut}_k k[u]$ determines $\mathrm{Aut}_k A$. Q.E.D.

3.1.6. COROLLARY. If the group $\mathrm{Aut}_k X$ for a k-form X of A^1 is finite of order not divisible by p, then $\mathrm{Aut}_k X$ is cyclic.

The corollary is clear from the natural split exact sequence $1 \longrightarrow k^+ \longrightarrow \mathrm{Aut}_k k[u] \longrightarrow k^\times \longrightarrow 1$, in view of 3.1.5.

3.1.7. Remark. No example is known to us of a k-form X of A^1 with finite, non-cyclic $\mathrm{Aut}_k(X)$.

3.2. We shall now turn to the quotient schemes of a k-form of A^1 under finite group action.

3.2.1. LEMMA. Let G be a finite group of k-automorphisms of a polynomial ring $k[t]$. Then, $k[t]^G$, the subring of invariant elements, is k-isomorphic to a polynomial ring $k[u]$.

Proof. Each $\sigma \in G$ is represented by a substitution $t \longmapsto t\sigma = a(\sigma)t + b(\sigma)$, and $\sigma \longmapsto a(\sigma) \in k^\times$ is a homomorphism of G onto a finite cyclic group of roots of unity in $k^\times$. Its kernel is the set of $\sigma \in G$ with $a(\sigma) = 1$, viz. translations, which forms a subgroup H of k^+ acting freely on Spec $k[t]$. It follows that $(\mathrm{Spec}\ k[t])/H \simeq A^1$ because it is a smooth quotient scheme of A^1. This means $k[t]^H \simeq k[u]$. Now the factor group G/H acts naturally on $(\mathrm{Spec}\ k[t])/H \simeq \mathrm{Spec}\ k[u]$, the H-orbit of the k-rational point $(t = 0)$ being a fixed point under the action. Let that point be $(u = c)$ with $c \in k$. If for $\bar{\sigma} \in G/H$ we have $u\bar{\sigma} = au + b$ then $(u - c)\bar{\sigma} = u\bar{\sigma} - c = au + b - (ac + b) = a(u - c)$. So, putting $w := u - c$, we realize the (G/H)-action on $k[w] = k[u]$ as being $w\bar{\sigma} = r(\bar{\sigma})w$ with $r(\bar{\sigma}) \in k^\times$ an n-th root of unity, $(p,n) = 1$. It is then clear that $k[w]^{G/H} = k[w^n] = k[u]^{G/H}$, a polynomial ring. Since $k[t]^G = (k[t]^H)^{G/H} = k[u]^{G/H}$, we see that our lemma is proven.

3.2.2. THEOREM. Let G be a finite group of k-automorphisms of a k-form X of A^1. Then, the quotient scheme X/G is a k-form of A^1.

Proof. Write $X = \operatorname{Spec} A$. G acts naturally on A and the action can be extended to $\bar{k} \otimes A$ in a natural fashion. Since $\bar{k} \otimes A^G \simeq (\bar{k} \otimes A)^G \simeq \bar{k}[t]^G \simeq \bar{k}[t]$ by the preceding lemma, $X/G = \operatorname{Spec} A^G$ is a k-form of A^1. Q.E.D.

3.3. In the following we shall show that if $p > 2$ then $|\mathrm{Aut}_k(X)| = 2$ for any hyperelliptic k-form X of A^1, and shall construct a k-form X of A^1 with $|\mathrm{Aut}_k(X)| = m$ for each characteristic $p > 2$ and positive integer m such that $(p,m) = (p, m + 1) = 1$.

3.3.1. PROPOSITION. *Assume* $p > 2$ *and* $k = k_s$. *Then,* $|\mathrm{Aut}_k(X)| = 2$ *for every hyperelliptic* k*-form* X *of* A^1.

Proof. By 2.2, X is birationally equivalent to an affine plane curve $y^2 = x^{p(m)} + a$ where $m \geq 1$ and $a \in k - k^p$. Then, by Chevalley [2; IV, §9, Th. 9], $k(x)$ is invariant under any birational k-automorphism of $k(X)$. Hence each automorphism $\sigma \in \mathrm{Aut}_k(X)$, restricted on the subfield $k(x)$, is written in the form:

$$\sigma(x) = (bx + c)/(dx + e) \quad \text{with} \quad b, c, d, e \in k.$$

Let $\alpha^{p(m)} = a$ with $\alpha \in \bar{k}$. Since σ fixes the point $(x,y) = (-\alpha,0)$, we have $d\alpha^2 + (b - e)\alpha - c = 0$. Since 1, α and α^2 are linearly independent over k, $d = c = 0$ and $b = e$. Hence $\sigma|_{k(x)}$ is the identity. Then we must have $(\sigma(y))^2 = y^2$. Hence $\sigma(y) = \pm y$. Since σ defined by $\sigma(x) = x$ and $\sigma(y) = -y$ is evidently an element of $\mathrm{Aut}_k(X)$, we conclude that $|\mathrm{Aut}_k(X)| = 2$. Q.E.D.

3.3.2. COROLLARY. Assume $p > 2$. Let G be a k-group of Russell type. Then, G is not a hyperelliptic curve.

The corollary is obvious from 3.3.1.

3.3.3. Let K be an algebraic function field of one variable over k, and let α be an element of $k^{1/p}$ not in k. Let $k' = k(\alpha)$ and $K' = k' \otimes K$. If σ is a birational k-automorphism of K, σ can be extended canonically to a birational k'-automorphism of K'. Let D be a k-trivial derivation of k' uniquely determined by the condition: $D(\alpha) = 1$. D can be extended canonically to a K-trivial derivation of K' by setting $D(\sum \lambda_i \otimes a_i) = \sum D(\lambda_i) \otimes a_i$ for $\sum \lambda_i \otimes a_i \in K'$. Thus we have the following

3.3.3.1. LEMMA. $\sigma D = D\sigma$.

Proof. For any element $\sum \lambda_i \otimes a_i$ of $k' \otimes K$, $(\sigma D)(\sum \lambda_i \otimes a_i) = \sum D(\lambda_i) \otimes \sigma(a_i) = (D\sigma)(\sum \lambda_i \otimes a_i)$.

3.3.4. THEOREM. Assume $p > 2$ and $k = k_s$. Let $m > 1$ be an integer not divisible by p, and let B be the affine plane curve

$$B : y^m = x^p + a \quad \text{with} \quad a \in k - k^p. \tag{1}$$

Then B is k-birationally equivalent to a k-form of A^1. If furthermore $m + 1$ is not divisible by p, then $|\mathrm{Aut}_k(k(B))| = m$.

Proof. We first show that B is k-birationally equivalent to a k-form of A^1. Note that B has a unique k-normal singular point $P : (x,y) = (-\alpha, 0)$ with $\alpha^p = a$. In case $p > m$, the homogeneous form of

(1) is

$$Y^m Z^{p-m} = X^p + aZ^p \tag{2}$$

where $y := Y/Z$ and $x := X/Z$. The point at infinity of the curve (2) is $Q : (X,Y,Z) = (0,1,0)$, which is a singular point if and only if $m < p - 1$. But even in case $m < p - 1$, it is not hard to show that Q is smoothable over k, that there lies only one point Q' over Q because $(p,m) = 1$, and that Q' is a smooth k-rational point. Let C be the k-normal completion of B. Since P is evidently a one-place point, $C - P$ is a k-form of A^1, which is not k-rational since P is a singular point. Next, in case $m > p$, the homogeneous form of the curve (1) is

$$Y^m = X^p Z^{m-p} + aZ^m \tag{3}$$

where $x := X/Z$ and $y := Y/Z$. The point at infinity of the curve (3) is $Q : (X,Y,Z) = (1,0,0)$, which is a singular point if and only if $m > p + 1$. If $m > p + 1$, Q is smoothable again over k and there exists only one point Q' over Q since $(p,m) = 1$. Q' is a smooth k-rational point. Therefore, $C - P$ is a non-rational k-form of A^1. In any case, B is birationally equivalent to a k-form of A^1. Observe that, if $m = p - 1$, $C - P$ is a Russell-type k-group $y^p = x - ax^p$.

We shall next show that, if $(p,m) = (p, m + 1) = 1$, then $|\mathrm{Aut}_k(k(B))| = m$. Let r and s be the positive integers such that $rm - sp = 1$, and let $t := (x + \alpha)^r / y^s$, where $a = \alpha^p$ with $\alpha \in k^{1/p}$. Then $y = t^p$ and $x + \alpha = t^m$. Let $k' := k(\alpha)$, $K := k(B)$ and $K' := k' \otimes K$. Then $K' = k'(t)$. Take any element σ of $\mathrm{Aut}_k(K)$, and extend σ to a birational

k'-automorphism of K'. Since $K' = k'(t)$ and σ fixes the point $P : (x,y) = (-\alpha,0)$, we may write $\sigma(t) = t/(\gamma t + \delta)$ with $\gamma, \delta \in k'$. As in 3.3.3, define a k-trivial derivation D of k' by $D(\alpha) = 1$, and extend it canonically to a K-trivial derivation of K'. Then $\sigma D = D\sigma$ by 3.3.3.1. From $x + \alpha = t^m$ follows $D(t) = rt^{-m+1}$. Now computing both sides of $\sigma D(t) = D\sigma(t)$, one obtains

$$r(\gamma t + \delta)^{m+1} = -\gamma' t^{m+1} - \delta' t^m + r\delta \qquad (4)$$

where $\gamma' := D(\gamma)$ and $\delta' := D(\delta)$. Because $(p, m + 1) = 1$, we have $r\gamma\delta^m = 0$ by comparison of coefficients of t in both sides of (4). Here, note that $\delta \neq 0$, for if otherwise σ would not be a birational k-automorphism. Hence $\gamma = 0$. Moreover the comparison of constant terms of (4) shows that $\delta^m = 1$. Because $(p,m) = 1$ and $k = k_s$, $\delta \in k$. Then, $\sigma(x) = \sigma(t^m - \alpha) = \delta^{-m}t^m - \alpha = t^m - \alpha = x$, and $\sigma(y) = \sigma(t^p) = \delta^{-p}t^p = \delta^{-p}y$. Now define a birational k-automorphism τ of B by $\tau(x) := x$ and $\tau(y) := \xi y$, where ξ is a primitive m-th root of unity. Then $\mathrm{Aut}_k(k(B))$ is certainly exhausted by $\{\tau^i \mid 0 \leq i \leq m\}$. Therefore $|\mathrm{Aut}_k(k(B))| = m$.

Q.E.D.

3.3.5. Remark. In the situation of 3.3.4, we have in fact:

(a) If $m + 1 = p^\ell n$ with $\ell \geq 1$, $(p,n) = 1$ and $n > 1$, then $|\mathrm{Aut}_k(k(B))| = n$.

(b) If $m + 1 = p^\ell$ with $\ell \geq 1$, then $\mathrm{Aut}_k(k(B))$ is isomorphic to a group $\mathcal{A} = \{(b,c,\delta) \mid b,c,\delta \in k,\ c = b^{p(\ell)} + a^{p(\ell)-1}c^{p(\ell)},$ and $\delta = \delta^{p(\ell)}\}$, where $(b,c,\delta)\cdot(b',c',\delta') := (b + b'\delta,\ c + c'\delta,\ \delta\delta')$, and

$\sigma(x) = (by^{p(\ell)-1} + \delta x)/(cy^{p(\ell)-1} + \delta)$ and $\sigma(y) = y/((b^p + c^p a)y + \delta^p)$ if $\sigma = (b,c,\delta)$. Since k is separably closed, $\mathrm{Aut}_k(k(B))$ is an infinite group. Therefore, B is birationally equivalent to an underlying scheme of a k-group of Russell type given by the equation $y^{p(\ell)} = x - a^{p(\ell)-1}x^{p(\ell)}$ (cf. KMT - 6.9.1).

(c) We have been unable to find a k-form X of A^1 such that $|\mathrm{Aut}_k(X)| = p^\ell - 1$.

3.3.6. PROPOSITION. *Assume* $p > 2$. *Let* C *be a projective plane curve*

$$C : X^pZ + aZ^{p+1} = Y^p(Y + aZ) \tag{5}$$

with $a \in k - k^p$. *Then* C *is a* k*-normal curve with only one singular point* $P : (X,Y,Z) = (-\alpha,0,1)$ *where* $\alpha^p = a$. *Moreover,* $C - P$ *is a non-rational* k*-form of* A^1, *and* $|\mathrm{Aut}_k(C)| = 1$.

Proof. Let $B : x^p + a = y^p(a + y)$ be an inhomogeneous form of C. The point P is given by $(x,y) = (-\alpha,0)$. Among the assertions, the first two are easily verified. So, we shall prove the last assertion only. Let $k' := k(\alpha)$, $K := k(C)$ and $K' = k' \otimes K$. Define a k-trivial derivation of k' by $D(\alpha) = 1$, and extend it canonically to a K-trivial derivation of K'. Let σ be an element of $\mathrm{Aut}_k(K)$, and extend it to a birational k'-automorphism of K'. Then $\sigma D = D\sigma$ by 3.3.3.1. Let $t := (x + \alpha - \alpha y)/y$. Then $x = -\alpha + \alpha t^p + t^{p+1}$ and $y = t^p$. Hence $D(t) = (1 - t^p)/t^p$. Since $\sigma(P) = P$, σ is written in the form $\sigma(t) = t/(\gamma t + \delta)$ with γ, $\delta \in k'$. Now, the computation of $\sigma D(t) = D\sigma(t)$ will give

$$\{\gamma^2(\gamma^p - 1) + \gamma'\}t^{p+2} + \{2\gamma\delta(\gamma^p - 1) + \delta'\}t^{p+1}$$
$$+ \delta\{(\gamma^p - 1)\delta + 1\}t^p + \delta^p\gamma^2t^2 + 2\gamma\delta^{p+1}t$$
$$+ \delta(\delta^{p+1} - 1) = 0. \qquad (6)$$

Since $p > 2$, from (6) follows $\gamma = 0$, if one notes $\delta \neq 0$. Moreover, we have $\delta = 1$ by calculating the coefficient of t^p in (6). Therefore, $\sigma(t) = t$, or σ is the identity. Therefore, $|\mathrm{Aut}_k(K)| = 1$. Q.E.D.

3.3.7. Remark. In case $p = 2$, the curve C defined by (5) is k-birationally equivalent to the Russell-type k-group (2) of KMT - 6.8.3; accordingly, $|\mathrm{Aut}_{k_s}(C)| = \infty$.

3.4. We showed in 3.3.1 above that if $p > 2$ a hyperelliptic (non-trivial) k-form of A^1 has exactly two birational k-automorphisms. However, the converse is false as shown by the following

Example. Let B be the affine plane curve

$$B : x^p + a = y^{2p}(a + y^2)$$

with $a \in k - k^p$. Then, as one can ascertain without difficulty, B is k-birationally equivalent to a k-form of A^1 and has exactly two birational k-automorphisms, viz. the identity automorphism and σ with $\sigma(x) = x$ and $\sigma(y) = -y$. Let $K := k(B)$. Then the subfield of elements of K invariant under $\mathrm{Aut}_k(K)$ is the function field of an affine plane curve

$$B_0 : x^p + a = y^p(y + a)$$

which is obviously not k-rational.

4. Divisor class groups and other invariants of the forms of the affine line.

4.0. Let X be a non-trivial k-form of the affine line $\mathbb{A}^1$ and let C be the k-normal completion of X in its function field over k. Assume throughout this section (§4) that X carries a k-rational point. Let $P_\infty := C - X$ and let $\mathcal{O}_\infty$ be the local ring of C at P_∞. By KMT - 6.7.9, $\mathcal{O}_\infty$ is smooth if and only if the arithmetic genus g of C is zero. P_∞ is not k-rational if $\mathcal{O}_\infty$ is singular (cf. 1.6.2). In this section, we are interested in the case in which the arithmetic genus g of C, viz. the k-genus of X, is positive. Then the connected component $\underline{\mathrm{Pic}}^0_{C/k}$ of the Picard scheme $\underline{\mathrm{Pic}}_{C/k}$ is a unipotent k-group of dimension g, and there is a closed immersion $i : X \hookrightarrow \underline{\mathrm{Pic}}^0_{C/k}$ defined by $i(Q) = Q - P_0$, where P_0 is a k-rational point on X (cf. KMT - 6.7.9).

In the following, we use these notations above and assume that the arithmetic genus g is positive.

Some preparatory results on Picard schemes and modules of differentials will be first given in this subsection 4.0.

4.0.1. LEMMA. *For every extension field k' of k, $C \otimes k'$ is a Gorenstein k'-scheme. In particular, $k' \otimes \mathcal{O}_\infty$ is a Gorenstein local ring.*

Proof. Since $\mathcal{O}_\infty$ is a regular local ring, it is a Gorenstein local ring. As all other points of C are smooth, C is a Gorenstein scheme of finite type defined over k. By [7; V, 9.4], $C \otimes k'$ is a Gorenstein scheme over k' for every extension field k' of k. Hence, the local ring of the point of $C \otimes k'$ lying over P_∞, namely $k' \otimes \mathcal{O}_\infty$, is a Gorenstein local ring.

4.0.2. Since $C \otimes k'$ is a Gorenstein k'-scheme, it has a dualizing sheaf $\underline{\omega}_{C \otimes k'/k'}$ which is a locally free $\mathcal{O}_{C \otimes k'}$-module of rank 1 —see [7] for the definitions and relevant facts. Among other things, the following natural isomorphisms are known to exist (cf. [7; III, (8.7) - (5)]):

$$\underline{\omega}_{C \otimes k'/k'} \simeq \mathcal{O}_{C \otimes k'} \otimes_{\mathcal{O}_C} \underline{\omega}_{C/k} \simeq k' \otimes \underline{\omega}_{C/k}. \tag{1}$$

Let $\overline{P}_\infty$ be the point of $C \otimes \overline{k}$ lying above P_∞, and let $\overline{o}_\infty$ be its local ring. Since the $\overline{k}$-normalization $\widetilde{C}$ of $C \otimes \overline{k}$ is isomorphic with $P^1_{\overline{k}}$, choose a global inhomogeneous parameter s of $P^1_{\overline{k}}$ so that the point $\widetilde{P}_\infty$ with local ring $\widetilde{o}_\infty$ lying over $\overline{P}_\infty$ is defined by $s = 0$. Then, $\underline{\omega}_{C \otimes \overline{k}/\overline{k}}$ is given as follows:

$$(\underline{\omega}_{C \otimes \overline{k}/\overline{k}})_P = \begin{cases} \Omega^1_{o/k} & \text{if } P \neq \overline{P}_\infty, \text{ where } o := \mathcal{O}_{P,\widetilde{C}} \\ \Omega' & \text{if } P = \overline{P}_\infty \end{cases} \tag{2}$$

where Ω' is the $\overline{o}_\infty$-module formed by all differentials $f.ds$ with $f \in \overline{k}(C)$ such that

$$\operatorname{Res}_{\widetilde{P}_\infty} (hf \cdot ds) = 0 \quad \text{for every } h \in \overline{o}_\infty. \tag{3}$$

For this fact, consult [20; p.78].

4.0.3. LEMMA. *In the notation of* 4.0.2, Ω' *is generated by* ds/s^d *as* $\overline{o}_\infty$*-module, where* d *is the degree of the conductor of* $\widetilde{o}_\infty$ *into* $\overline{o}_\infty$.

Proof. d is the smallest positive integer such that $s^{d-1} \notin \overline{o}_\infty$ and

$s^n \in \overline{o}_\infty$ whenever $n \geq d$. Then $ds/s^d \in \Omega'$ and $\mathrm{Res}_{\widetilde{P}_\infty}(s^{n-1}ds/s^n) = 1$ if $n > d$. Since $\underline{\omega}_{C \otimes \overline{k}/\overline{k}}$ is a locally free sheaf of rank 1, $\Omega' = \overline{o}_\infty \cdot (ds/s^m)$ for some $m > 0$. Hence $ds/s^d = f\, ds/s^m$ with $f \in \overline{o}_\infty$. The remark above implies that $m = d$. Therefore $\Omega' = \overline{o}_\infty \cdot (ds/s^d)$. Q.E.D.

4.0.4. For any extension field k' of k, let $\omega_{C/k'} := \Gamma(C \otimes k', \underline{\omega}_{C \otimes k'/k'})$. Then $\omega_{C/k'} = k' \otimes \omega_{C/k}$, and $\omega_{C/k}$ is a k-vector space of dimension equal to the arithmetic genus g of C, called the space of Weil differentials of the first kind of C. From what we observed in 4.0.2, every element of $\omega_{C/k}$ is regular on $X = C - P_\infty$.

4.0.5. PROPOSITION. $\underline{\mathrm{Pic}}^0_{C \otimes \overline{k}/\overline{k}}$ is $\overline{k}$-isomorphic with the generalized Jacobian variety J' of $P^1_{\overline{k}}$ with the equivalence relation defined by $\overline{o}_\infty$, the local ring of $C \otimes \overline{k}$ at $\overline{P}_\infty$.

Proof. Let $\overline{C} := C \otimes \overline{k}$ and $\phi : \widetilde{C} \simeq P^1_{\overline{k}} \longrightarrow \overline{C}$ the $\overline{k}$-normalization of $\overline{C}$. In the exact sequence

$$1 \longrightarrow \phi^*(\mathcal{O}^\times_{\overline{C}}) \longrightarrow \mathcal{O}^\times_{\widetilde{C}} \longrightarrow S \longrightarrow 1 \qquad (4)$$

of sheaves of abelian groups over $\widetilde{C} \simeq P^1_{\overline{k}}$, the cokernel S is concentrated at the point $\widetilde{P}_\infty$. From (4) arises an exact sequence

$$1 \longrightarrow H^0(\widetilde{C}, \phi^*(\mathcal{O}^\times_{\overline{C}})) \longrightarrow H^0(\widetilde{C}, \mathcal{O}^\times_{\widetilde{C}}) \longrightarrow H^0(\widetilde{C}, S)$$
$$\longrightarrow H^1(\widetilde{C}, \phi^*(\mathcal{O}^\times_{\overline{C}})) \longrightarrow H^1(\widetilde{C}, \mathcal{O}^\times_{\widetilde{C}}) \longrightarrow 1$$

or $1 \longrightarrow \overline{k}^\times \longrightarrow \overline{k}^\times \longrightarrow \widetilde{o}^\times_\infty/\overline{o}^\times_\infty \longrightarrow \mathrm{Pic}\ \overline{C} \longrightarrow Z \longrightarrow 1$ in the usual manner. Therefore, $\mathrm{Pic}^0\overline{C} \simeq \underline{\mathrm{Pic}}^0_{\overline{C}/\overline{k}}(\overline{k}) \simeq \underline{\mathrm{Pic}}^0_{C/k}(\overline{k}) \simeq \widetilde{o}^\times_\infty/\overline{o}^\times_\infty$ holds. Since every divisor

of degree 0 on $\tilde{C}(\simeq P^1_{\bar{k}})$ is linearly equivalent to div(f) for some $f \in \tilde{o}_\infty^\times$, the last isomorphism shows that the $\bar{k}$-rational points $\underline{\mathrm{Pic}}^0_{C/\bar{k}}(\bar{k})$ is identifiable with the generalized Jacobian variety on $P^1_{\bar{k}}$ defined by $\bar{o}_\infty$. $\underline{\mathrm{Pic}}^0_{C/\bar{k}}$, as it is known to be smooth, is consequently identifiable with the said generalized Jacobian variety. Q.E.D.

4.0.5.1. Remark. This proposition 4.0.5 rectifies the erroneous assertion on page 81 of KMT, made in the course of the proof of 6.7.6 but not actually used there.

4.0.6. Take a k-rational point P_0 from $C - P_\infty$, and consider the imbedding $i : C - P_\infty \hookrightarrow \underline{\mathrm{Pic}}^0_{C/k}$ as in 4.0 above. The following result is proved in [20; p. 97] in a slightly more restrictive situation.

4.0.6.1. LEMMA. Let Ω be the space of invariant differentials on $\underline{\mathrm{Pic}}^0_{C/k}$. Then, the imbedding $i : C - P_\infty \hookrightarrow \underline{\mathrm{Pic}}^0_{C/k}$ induces an isomorphism $i^* : \Omega \xrightarrow{\sim} \omega_{C/k}$, $\omega_{C/k}$ being the space of Weil differentials of the first kind on C (cf. 4.0.4).

Proof. To prove that the k-linear mapping $i^* : \Omega \longrightarrow \omega_{C/k}$ is an isomorphism, it is enough to show that $\bar{k} \otimes i^* : \bar{k} \otimes \Omega \longrightarrow \bar{k} \otimes \omega_{C/k} \simeq \omega_{C/\bar{k}}$ is an isomorphism. As $\bar{k} \otimes i^* = (i \otimes \bar{k})^*$ and $\underline{\mathrm{Pic}}^0_{C/\bar{k}}$ is identified with a generalized Jacobian variety J' of $P^1_{\bar{k}}$ as in 4.0.5, we may, and shall, proceed to prove our assertion under the assumption that $k = \bar{k}$ and $\underline{\mathrm{Pic}}^0_{C/k} = J'$. We follow up the proof of Serre [20; Chap. V, Prop. 5, p. 97].

Let $X = C - P_\infty$, let $\phi : X^g \longrightarrow J'$ be the morphism $\phi(x_1, \ldots, x_g) = \sum_{j=1}^g i(x_j)$ and let $h_j : X^g \longrightarrow J'$ be the morphism

$h_j(x_1, \ldots, x_g) = i(x_j)$. Then $\phi = \sum_{j=1}^{g} h_j$ and $\phi^*(\omega) = \sum h_j^*(\omega)$ for any element ω of Ω. Hence if $i^*(\omega) = 0$ then $\phi^*(\omega) = 0$. Meanwhile, the morphism $\phi : X^g \longrightarrow J'$ is decomposed as a composite of morphisms $X^g \xrightarrow{\psi} X^{(g)} \xrightarrow{\rho} J'$, where $X^{(g)}$ is the symmetric product of g copies of X. Since ψ and ρ are generically separable and dominating, $\phi^*(\omega) = 0$ implies $\omega = 0$. Therefore, the mapping $\omega \longmapsto i^*(\omega)$ is injective; it is then surjective because $\mathrm{kim}_k\Omega = \dim_k \omega_{C/k} = \dim H^1(C, \mathcal{O}_C) = g$. There remains for us to show that $i^*(\omega) \in \omega_{C/k}$ if $\omega \in \Omega$. For this, by virtue of [20; IV, n°9, Prop. 6], we have only to show that $\mathrm{Tr}_a(i^*(\omega)) = 0$ for every rational function $a \in o_\infty$, $a \notin K^p$, where $K = k(C)$. Let $h = \mathrm{Tr}_a(i)$ be the rational mapping from P^1 to J' defined in [20; III, n°2]. By [20; III, n°6, Lemma 4 and its remark], $\mathrm{Tr}_a(i^*(\omega)) = h^*(\omega)$. On the other hand, it is obvious that $i(\mathrm{div}(b)) = 0$ if $b \in o_\infty$. Therefore, on the basis of [20; III, Prop. 9] slightly modified, we conclude that h is a constant mapping. Hence $h^*(\omega) = 0$. Q.E.D.

4.1. We now introduce various invariants attached to k-forms of A^1. Let $X = \mathrm{Spec}\ A$ be a k-form of A^1 and C a complete k-normal model of the function field $K = k(X)$. Let $K' = k(x)$ be the unique maximal rational subfield of K over which K is purely inseparable, and let $A' = k[u]$ be the unique maximal polynomial subring over which A is purely inseparable. (See 1.5.2 for the existence of K' and A'.) Let $\gamma : C \longrightarrow P^1_k$ be the morphism afforded by the inclusion $K' \hookleftarrow K$, and put $P'_\infty := \gamma(P_\infty)$ where $P_\infty = C - X$. Call o_∞, o'_∞ the places corresponding to P_∞, P'_∞, respectively. Let finally $\tilde{o}_\infty$ denote the integral closure of o_∞ in

$k \otimes K$. We put now:

$$(*)\quad \begin{cases} \lambda := \mathrm{ht}(X) = \text{the height of } X \quad (\text{cf. } 1.1) \\ \lambda' := \mathrm{ht}(K) = \text{the height of } K \quad (\text{cf. } 1.2) \\ p^{\varepsilon} := [k(P'_\infty) : k] = \text{the degree of } P'_\infty \\ p^{\eta} := e(o_\infty : o'_\infty) = \text{the ramification index of } o_\infty \text{ over } o'_\infty \\ p^{\nu} := e(\tilde{o}_\infty : o_\infty) = \text{the ramification index of } \tilde{o}_\infty \text{ over } o_\infty \end{cases}$$

PROPOSITION. (a) $\lambda = \lambda' + \varepsilon$ with $k(u) = k(x^{p(\varepsilon)})$; (b) $\lambda = \eta + \nu$; (c) $p^{\nu} = [k(P_\infty) : k]$; (d) $\lambda \geq \nu \geq \lambda - \lambda'$.

Proof. (a) In the proof of 1.5.2, one saw already that $K' = k(x)$, $A' = k[A^{p(\lambda)}]$, $k(u) = k(x^{p(\delta)})$ and $\lambda = \lambda' + \delta$ for $\delta \geq 0$. On the other hand, $P^1_k - P'_\infty$ is a k-rational k-form of A^1 whose height equals $\varepsilon = \deg(P'_\infty)$ by KMT - 6.8.1. Therefore, $\varepsilon = \delta$ follows.

(b) Let $\tilde{o}'_\infty$ be the integral closure of o'_∞ in $\bar{k} \otimes K'$. Then, if one writes $K' = k(t)$ with a suitable t, the place o'_∞ corresponds to $t^{p(\varepsilon)} - a$ with $a \in k - k^p$, so $\tilde{o}'_\infty$ is given by $t - a^{p(-\varepsilon)}$. Hence, $p^{\varepsilon} = e(\tilde{o}'_\infty : o'_\infty)$ obtains. Also, $p^{\lambda'} = [K : K'] = [\bar{k} \otimes K : \bar{k} \otimes K'] = e(\tilde{o}_\infty : \tilde{o}'_\infty)$, because $f(\tilde{o}_\infty : \tilde{o}'_\infty) = 1$ obviously. Consequently, $p^{\nu} \cdot p^{\eta} = e(\tilde{o}_\infty : o'_\infty) = e(\tilde{o}_\infty : \tilde{o}'_\infty) e(\tilde{o}'_\infty : o'_\infty) = p^{\lambda'} \cdot p^{\varepsilon}$, and $\nu + \eta = \lambda' + \varepsilon$ is proven.

(c) $[k(P_\infty) : k] = [k(P_\infty) : k(P'_\infty)] \cdot [k(P'_\infty) : k] = [K : K'] \cdot p^{-\eta} \cdot p^{\varepsilon}$ $= p^{\lambda' - \eta + \varepsilon} = p^{\nu}$.

(d) Clear from (c) and the definition of ε.

4.2. For $X = \mathrm{Spec}\, A$ as in 4.1, we define one more invariant:

μ := the p-exponent of the divisor class group $C(A) = \mathrm{Pic}\, X$ of A (cf. KMT - 6.10.1).

THEOREM. $\lambda = \mu \geq \nu$.

A proof of this theorem will be given in the next three paragraphs 4.2.1 - 4.2.3.

4.2.1. LEMMA. Let o be a smooth place of K/k, and let $o_1 := k^{1/p} \otimes o$. Then, $e(o_1 : o) = 1$ if and only if o is k-rational.

Proof. Let $k' \subseteq k^{1/p}$ be a finite extension of k such that $e(k' \otimes o : o) = e(o_1 : o)$, and write $o' := k' \otimes o$, k' := the residue field of o', k := the residue field of o. We have $[k' : k] = [k' : k'][k' : k] = [k' : k']e(o' : o)f(o' : o) = [k' : k][k : k] = f(o' : o)[k : k]$, whence follows

$$[k' : k']e(o' : o) = [k : k].$$

Thus, if $e(o' : o) = e(o_1 : o) > 1$, then o is non- k-rational. (Observe that $e(o_1 : o)$ is either 1 or p, clearly.) Next, suppose $e(o_1 : o) = 1$. As k' is isomorphic as k-algebra with $k' \otimes k$ modulo its nilradical, we have

$$[k' : k] = [k' \otimes k : k] \geq [k' : k] = f(o' : o).$$

But $[k' : k] = f(o' : o)$, which shows that the last inequality is actually an equality, and $k' \simeq k' \otimes k$. If $k \supset k$, choose k' so that $k' \cap k \supset k$; then $k' \otimes k$ would have a nonzero nilradical, contradicting the last

isomorphism. Therefore, $k = k$ and o is k-rational. Q.E.D.

4.2.2. PROPOSITION. $p^{\lambda} \geq p^{\mu}$.

Proof. For each $1 \leq i \leq \lambda$, let $k_i := k^{p(-i)}$, let $X_i := X \otimes k_i$, and let C_i be the normalization of C in $K_i := k_i \otimes K$, where K denotes $k(X)$. Further, let P_i be the point of C_i lying over P_∞ of C. Since X_λ is k_λ-isomorphic to A^1, P_λ is k_λ-rational. Let Q be an arbitrary point on X, and for $1 \leq i \leq \lambda$ let Q_i be the point of $X \otimes k_i$ lying over Q. Suppose first that Q is k-rational. One can find an inhomogeneous parameter t on $P^1_{k_\lambda}$, such that $t = 0$ at Q_λ and $t = \infty$ at P_λ. Since $t^{p(\lambda)} \in K$, we have a linear equivalence $p^{\lambda}Q \sim p^{\lambda-\nu}P_\infty$ (clearly, $\lambda \geq \nu$). Therefore the divisor class of $C(A)$ represented by k-rational point Q is annihilated by p^{λ}. Next, if Q is not a k-rational point, let o be the local ring of Q and let o_i be the local ring of Q_i; we know by 4.2.1 that Q_i is non-k_i-rational if and only if the ramification index $e(o_{i+1} : o_i)$ equals p. Therefore, if we call r the smallest positive integer such that Q_r is a k_r-rational point, and if $\lambda \geq r$, then $p^{\lambda-r}Q \sim p^{\lambda-\nu}P_\infty$ by an argument similar to the preceding one; if on the other hand $r > \lambda$, $Q_\lambda \sim p^{r-\lambda}Q'$ with a k_λ-rational point Q'_λ lying over a k-rational point Q' of X. Hence $Q \sim p^{r}Q' \sim p^{r-\nu}P_\infty$. Therefore, in each case the divisor class of $C(A)$ represented by a point Q is annihilated by p^{λ}.

4.2.3. PROPOSITION. $p^{\mu} \geq p^{\lambda}$.

Proof. Let $f : k \longrightarrow k$ be the Frobenius endomorphism, and let

$A^{[i]} := A^{(p^i)} := (k, f^i) \otimes A$, which we can identify with a k-subalgebra of $A^{[j]}$ for each $0 \leq j < i$ by means of 0.3.1, repeated. In particular, we shall consider $A^{[i]} \simeq k[A^{p(i)}] \subseteq A$. Let P be a k-rational point of X, and call p the prime ideal of A corresponding to P. Let $p_i := p \cap A^{[i]}$. Then, since the divisor class of C(A) represented by P is annihilated by p^μ, it is not hard to show that $p_\mu A = p^{p(\mu)}$ is a principal ideal. Write $p_\mu A = \xi A$.

We shall show that $\xi \in A^{[\mu]}$. In fact, consider $\overline{A} := \overline{k} \otimes A$; then $\overline{A} = \overline{k}[t]$ for some element t of $\overline{A}$, and $\overline{A}^{[i]} = \overline{k} \otimes A^{[i]} = \overline{k}[t^{p(i)}]$. Moreover, as can be verified at once, $p\overline{A}$ and $p_i\overline{A}^{[i]}$ are maximal ideals of $\overline{A}$ and $\overline{A}^{[i]}$, respectively. We may therefore assume that $p\overline{A} = t\overline{A}$. Since $e(A_p : A^{[i]}_{p_i}) = p^i$, we know that $\xi = \alpha t^{p(\mu)}$ with $\alpha \in \overline{k}$. Hence $\xi \in \overline{A}^{[\mu]} \cap K = A^{[\mu]}$. Since A is a faithfully flat $A^{[\mu]}$-module, this implies that $p_\mu = \xi A^{[\mu]}$. Let $C^{(\mu)}$ be a complete k-normal model of $X^{[\mu]} := \operatorname{Spec} A^{[\mu]}$, and let $P_\infty^{(\mu)}$ be its point at infinity. Then, $p_\mu = \xi A^{[\mu]}$ implies that point P_μ of $C^{(\mu)}$ corresponding to p_μ is linearly equivalent to $P_\infty^{(\mu)}$ over k. Consequently, $P_\infty^{(\mu)}$ is a k-rational point. Therefore $X^{[\mu]} = C^{(\mu)} - P_\infty^{(\mu)}$ is a trivial k-form of A^1. By 0.3.2, it follows that $p^\mu \geq p^\lambda$.

The preceding two inequalities show $\lambda = \mu$, while $\lambda \geq \nu$ is apparent from Proposition 4.1. Theorem 4.2 has thus been established as true.

4.2.4. Example (in which $\lambda = 2$, $\lambda' = \nu = 1$). Let C be the projective plane curve defined by

$$Y^pZ - aZ^{p+1} = X^p(Y + X)$$

with $a \in k - k^p$. Then C is a k-normal curve with only one singular point $P_\infty = (0,a^{1/p},1)$. Let $X = C - P_\infty$. Then X is a non-trivial k-form of A^1 with $\lambda = 2$ and $\nu = 1$. Indeed: it is straightforward to affirm that C is a k-normal curve with only one singular point $(0,a^{1/p},1)$. Now setting $x := X/Z$ and $y := Y/Z$, we have

$$y^p - a = x^p(y + x).$$

P_∞ is given by $(x,y) = (0,\alpha)$ with $\alpha^p = a$. Let $y - \alpha = xt$. Then we have

$$t^p - \alpha = x(1 + t). \tag{5}$$

It is now immediate to show that there exists only one point $(x,t) = (0,\alpha^{1/p})$ over P_∞, which is a smooth point of the curve (5). Hence X is a nontrivial k-form of A^1, and $\nu = 1$ and $\lambda = 2$. Evidently $\lambda' = 1$ in this example.

4.2.5. Example (in which $\lambda = \nu = 2$, $\lambda' = 1$). Let C be a normal projective plane curve defined by

$$X^pZ + aZ^{p+1} = (Y^p - bZ^p)(X + Y)$$

with both a, $b \in k - k^p$ and $a \neq b$. C has only one singular point $P_\infty = (-a^{1/p},b^{1/p},1)$. Let $X := C - P_\infty$. Then X has $\lambda = \nu = 2$, $\lambda' = 1$. Indeed: Let $x := X/Z$ and $y := Y/Z$. Then we have

$$x^p + a = (y^p - b)(x + y).$$

Let $\alpha^p = a$ and $\beta^p = b$ with α and $\beta \in k^{1/p}$. Setting $x + \alpha := (y - \beta)t$ we have

$$(1 + t)y = \alpha + \beta t + t^p.$$

Therefore X is $k^{1/p}$-rational, and $(y,t) = (\beta,(\beta - \alpha)^{1/p})$ is the only point lying over P_∞. It is now clear that $\lambda = \nu = 2$ and $\lambda' = 1$ in view of Proposition 4.1.

4.2.6. Example (in which $\lambda = \lambda' = 2$, $\nu = 1$). Let X be a k-group of Russell type given by

$$y^{p(2)} = x + ax^p \quad (p > 2, \quad a \in k - k^p).$$

For this X, $\lambda = 2$ by KMT - 2.7ff and $\lambda' = 2$ by 3.1.3. As in §2, we blow up the point at infinity of X p-times in succession (details are omitted), thereby verifying that $k(P_\infty) = k(a^{1/p})$ in the notation of 4.1. Therefore, by Proposition 4.1(c), $\nu = 1$.

4.3. Let $X = \operatorname{Spec} A$ be a nontrivial k-form of A^1, and let $X_i := X \otimes k^{p(-i)}$, $C_i :=$ the $k^{p(-i)}$-normal completion of X_i. Let $P_i := C_i - X_i$ with local ring $o_i \subseteq k^{p(-i)}(C_i)$. With the notations as these and also as in 4.1, we have

4.3.1. PROPOSITION. The following are equivalent:

(a) $\lambda = \nu$;

(b) $e(o_{i+1} : o_i) = \begin{cases} p & \text{for } 0 \le i \le \nu \\ 1 & \text{for } \nu \le i. \end{cases}$

Proof. (a)$\Rightarrow$(b) : Since X_λ is $k^{p(-\lambda)}$-isomorphic to A^1, P_λ is $k^{p(-\lambda)}$-rational. Therefore, by 4.2.1, $e(o_{i+1} : o_i) = 1$ if $i \geq \lambda$. Then $e(o_{i+1} : o_i)$ should equal p for $0 \leq i \leq \nu$, given that $p^\lambda = p^\nu$.

(b)$\Rightarrow$(a): In view of the assumption and Proposition 4.1(c), one can find a finite extension field k' of k such that $k \subseteq k(P_\infty) \subseteq k' \subseteq k^{p(-\nu)}$ and also that the place P'_∞ at infinity of $X \otimes k'$ has ramification index p^ν over P_∞ (this last due to $e(o_\nu : o_\infty) = p^\nu$). Put $d := [k' : k]$ and call o'_∞ the valuation ring of P'_∞. Since $[k' \otimes K : K] = d$ and $e(o'_\infty : o_\infty) = p^\nu$, it follows that $f(o'_\infty : o_\infty) = d \cdot p^{-\nu}$. But $[k(P_\infty) : k] = p^\nu$ and $[k' : k] = d$, so $[k' : k(P_\infty)] = d \cdot p^{-\nu}$, too. Therefore, $k'(P'_\infty) = k'$ and P'_∞ is smooth. Then P_ν which dominates P'_∞, too, is smooth and $X \otimes k^{p(-\nu)}$ is isomorphic to A^1 over $k^{p(-\nu)}$. So, $\nu \geq \lambda$, whence $\nu = \lambda$. Q.E.D.

4.3.2. PROPOSITION. Let $C^0(A)$ be the subgroup of $C(A)$ consisting of divisor classes on X of degree zero, and let $\rho : \mathrm{Pic}(C) \longrightarrow \mathrm{Pic}(X) = C(A)$ be the canonical restriction map (cf. KMT - 6.10.1). Then we have:

(a) $0 \longrightarrow C^0(A) \longrightarrow C(A) \xrightarrow{d} Z/p^\lambda Z \longrightarrow 0$ is an exact sequence.

(b) $C^0(A) \leq (\mathrm{Pic}^0_{C/k}(k))$ and $\rho(\mathrm{Pic}^0_{C/k}(k))/C^0(A) \simeq Z/p^{\lambda-\nu}Z$.

Proof. Let P_0 be a k-rational point of X. By the proof of 4.2.2, p^λ is then the smallest integer such that $p^\lambda P_0 \sim 0$ on X. Since every point on X linearly equivalent to an integral multiple of P_0 modulo divisors of degree zero, we have an exact sequence,

$$0 \longrightarrow C^0(A) \longrightarrow C(A) \xrightarrow{d} Z/p^\lambda Z \longrightarrow 0$$

where d is defined in such a way that $d(D) = n$ if D is linearly equivalent to nP_0 modulo a divisor of degree zero. Next, it is clear that $C^0(A) \subseteq \rho(\underline{\mathrm{Pic}}^0_{C/k}(k))$. Moreover, since $p^\nu P_0 - P_\infty$ represents an element of $\underline{\mathrm{Pic}}^0_{C/k}(k)$, $\rho(\underline{\mathrm{Pic}}^0_{C/k}(k))$ is generated by the divisor class of $\rho(p^\nu P_0 - P_\infty) = p^\nu P_0$ modulo $C^0(A)$. Thence follows the second assertion.

Q.E.D.

4.3.3. COROLLARY. The following are equivalent:

(a) $\lambda = \nu$.

(b) $\rho(\underline{\mathrm{Pic}}^0_{C/k}(k)) = C^0(A)$.

4.4. Let us for now restrict our attention to the forms of height one. Thus, X is a k-form of A^1, with k-normal completion C, for which $\lambda = 1$ in the notaion of 4.1. We continue to treat the forms X whose k-genus $g > 0$. By Theorem 4.2, $\underline{\mathrm{Pic}}^0_{C/k}$ is a commutative unipotent k-group of p-exponent 1; it is therefore a k-form of the g-dimensional vector group G_a^g. Such k-forms have been completely described in KMT - §2. Among other things, the affine algebra B of $\underline{\mathrm{Pic}}^0_{C/k}$ is generated by $2g$ elements $x_1, \ldots, x_g; y_1, \ldots, y_g$ which are subject to the following relations:

$$y_i^p = \sum_{j=1}^g a_{ij}x_j + \phi_i(x_1^p, \ldots, x_g^p) \quad (1 \le i \le g) \tag{6}$$

where $a_{ij} \in k$ such that $\det(a_{ij}) \neq 0$ and $\phi_i(x_1^p, \ldots, x_g^p)$ is a p-polynomial in $x_1^p, \ldots, x_g^p$ with coefficients in k. The group law on $\underline{\mathrm{Pic}}^0_{C/k}$ is defined by the comultiplication $\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i$ and

$\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i$ for $1 \leq i \leq g$. Since $\det(a_{ij}) \neq 0$, we have $dx_1 = \ldots = dx_g = 0$ in $\Omega^1_{B/k}$. Therefore $dy_1, \ldots, dy_g$ are invariant differentials on $\underline{\mathrm{Pic}}^0_{C/k}$. In the notation of 4.0, let $z_j := i^*(y_j)$ for $1 \leq i \leq g$, and let t be an inhomogeneous parameter on P^1 over $k^{1/p}$ such that t is finite on $X \otimes k^{1/p}$ and $t = \infty$ at P_∞. With these notations, we have

PROPOSITION. *Let* $X = \mathrm{Spec}\ A$ *be a* k*-form of* A^1 *of height* 1. *Then* A *is generated by* $t^p, z_1, \ldots, z_g$ *over* k, *viz.* $A = k[t^p, z_1, \ldots, z_g]$. *Moreover,* $dz_1, \ldots, dz_g$ *form a basis of* $\omega_{C/k}$.

Proof. Let B be the affine algebra of $\underline{\mathrm{Pic}}^0_{C/k}$. Then $i : X \hookrightarrow \underline{\mathrm{Pic}}^0_{C/k}$ induces an onto homomorphism $\rho : B \longrightarrow A$. Let $w_j = i^*(x_j)$ for $1 \leq j \leq g$. Then, as the above relation (6) implies $x_j \in (k^{1/p} \otimes B)^p$, we have $w_j \in (k^{1/p} \otimes A)^p$. Since $k^{1/p} \otimes A = k^{1/p}[t]$, it follows that $w_j \in k[t^p]$. But $A = k[z_1, \ldots, z_g, w_1, \ldots, w_g]$, whence $A = k[t^p, z_1, \ldots, z_g]$. The second statement follows from Lemma 4.0.6.1.

4.5. Returning to k-forms of A^1 of arbitrary height, we shall examine Frobenius morphisms. Let X be a k-form of A^1 of k-genus $g > 0$, let C be a k-normal completion of X and let $P_\infty = C - X$. For any k-scheme Y, we denote by $Y^{(p)}$ the k-scheme $Y \otimes (f,k)$, $f : k \longrightarrow k$ being the p-th power map of k, and by $F_Y : Y \longrightarrow Y^{(p)}$ the Frobenius k-morphism of Y. If G is a commutative k-group scheme, "the multiplication by p" endomorphism of G is factored into a composite of k-homomorphisms: $G \xrightarrow{F_G} G^{(p)} \xrightarrow{V_G} G$. V_G is called the Verschiebung of G. It is well-known that G is smooth over k if and only if F_G is faithfully flat

(cf. KMT - 1.4). V_G is in that case uniquely determined: namely, if V' is a k-homomorphism $G^{(p)} \longrightarrow G$ such that $V' \cdot F_G = p$, then $V' = V_G$.

Let $\underline{\mathrm{Pic}}^0_{C/k}$ be the connected component of the Picard schme of C. We denote by F_G the Frobenius k-homomorphism $\underline{\mathrm{Pic}}^0_{C/k} \longrightarrow (\underline{\mathrm{Pic}}^0_{C/k})^{(p)}$. Let $i : X \hookrightarrow \underline{\mathrm{Pic}}^0_{C/k}$ be the imbedding defined in 4.0 by means of a fixed k-rational point P_0 on X. Then we have the following obvious

4.5.1. LEMMA. The following diagram is commutative:

$$\begin{array}{ccc} X & \xrightarrow{\ i\ } & \underline{\mathrm{Pic}}^0_{C/k} \\ {\scriptstyle F_X}\downarrow & & \downarrow{\scriptstyle F_G} \\ X^{(p)} & \xrightarrow{\ i^{(p)}\ } & (\underline{\mathrm{Pic}}^0_{C/k})^{(p)} \end{array}$$

where $i^{(p)} := i \otimes (f,k)$. F_G is faithfully flat.

4.5.2. Let C' be the complete k-normalization of $X^{(p)}$ in the function field of $C^{(p)}$. Then $F_C : C \longrightarrow C^{(p)}$ decomposes into a composite: $C \xrightarrow{\phi} C' \xrightarrow{\psi} C^{(p)}$. ϕ and ψ cause k-homomorphisms of Picard schemes: $\psi_0 : \underline{\mathrm{Pic}}^0_{C^{(p)}/k} \simeq (\underline{\mathrm{Pic}}^0_{C/k})^{(p)} \longrightarrow \underline{\mathrm{Pic}}^0_{C'/k}$ and $\phi_0 : \underline{\mathrm{Pic}}^0_{C'/k} \longrightarrow \underline{\mathrm{Pic}}^0_{C/k}$. Let $P'_\infty := \phi(P_\infty)$ and $P''_\infty := \psi(P'_\infty)$. Then, $C' - P'_\infty$ is k-isomorphic to $C^{(p)} - P''_\infty$. Let $P'_0 := \phi(P_0)$ and $P''_0 := \psi(P'_0)$. The imbedding $i^{(p)}$ is in fact defined by $i^{(p)}(Q'') := Q'' - P''_0$ for a point Q'' on $X^{(p)}$ rational over any extension field k' of k. The k-rational point P'_0 defines a k-morphism $i' : X^{(p)} \longrightarrow \underline{\mathrm{Pic}}^0_{C'/k}$, which is given by $i'(Q') := Q' - P'_0$ for any point Q' on $X^{(p)}$, rational over any extension field k' of k. i' is an imbedding if the arithmetic genus g' of C' is positive, but i' is

a zero map if $g' = 0$. Evidently, we have $i' = \psi_0 \cdot i^{(p)}$. We claim that $\phi_0 \cdot \psi_0$ is the Verschiebung V_G of $G := \underline{\mathrm{Pic}}^0_{C/k}$. This assertion follows from the following general fact, inasmuch as $\phi_0 \cdot \psi_0 = \underline{\mathrm{Pic}}^0_{C/k}(F_C)$.

LEMMA. For any complete normal k-curve C with Picard scheme $G = \underline{\mathrm{Pic}}^0_{C/k}$, it holds that $G(F_C) = V_G$.

Proof. It suffices for our purpose to prove that $G(F_C)F_G$ is the multiplication by p map $p \cdot id_G$, in view of remark 4.5. In fact, enough to prove that assuming $k = k_s$. Let U be an open dense subset of smooth k-rational points on C such that the canonical rational map $i : C \longrightarrow G$ is defined on U. Thus, $i : U \longrightarrow G$ and $i^{(p)} : U^{(p)} \longrightarrow G^{(p)}$. Then, for any $Q \in U$, $F_C^{-1}(Q) = pQ$ as divisors on C, $C^{(p)}$. Therefore, $p \cdot i(Q) = G(F_C) \cdot i^{(p)} \cdot F_C(Q) = G(F_C) \cdot F_G(i(Q))$. So, $p \cdot id_G$ and $G(F_C) \cdot F_G$ agree on the subset $i(U)$ which generates a dense subgroup of $G(k)$. Hence $p \cdot id_G = G(F_C) \cdot F_G$.

4.5.3. LEMMA. Let C be a k-normal completion of a k-form X of A^1, and let $G := \underline{\mathrm{Pic}}^0_{C/k}$. Let H be the kernel of the endomorphism $p \cdot id_G : G \longrightarrow G$ defined by $x \longmapsto x + \ldots + x$ (p times). Then, H is geometrically connected.

Proof. Since $H \otimes \overline{k}$ is identifiable as the kernel of $p \cdot id_{\overline{G}}$ on $\overline{G} := \underline{\mathrm{Pic}}^0_{C/k} \otimes \overline{k} \simeq \underline{\mathrm{Pic}}^0_{C \otimes \overline{k}/\overline{k}}$, we have only to show that $H(\overline{k})$ is connected. Hence, replacing C by $C \otimes \overline{k}$, we shall assume in this proof that k is algebraically closed. C is then not normal. The normalization $\widetilde{C}$ of C is isomorphic to P^1_k. Let $\widetilde{P}_\infty$ be the point of $\widetilde{C}$ lying over P_∞, and

choose an inhomogeneous parameter s on P^1_k such that $s = 0$ at $\tilde{P}_\infty$. Let $\tilde{o}$ and o be the local rings of $\tilde{P}_\infty$ and P_∞, respectively. Let us define the multiplicative groups $\tilde{U}$ and U by

$$\tilde{U} = \{f \in \tilde{o} \ ; \ f(\tilde{P}_\infty) = 1\} \quad \text{and} \quad U = \{f \in o \ ; \ f(P_\infty) = 1\}.$$

Then U is a subgroup of $\tilde{U}$. It is clear from the proof of 4.0.5 that $\underline{\mathrm{Pic}}^0_{C/k}(k)$ is isomorphic to $\tilde{U}/U$.

Let $\hat{\tilde{o}}$ and $\hat{o}$ be respectively the completions of $\tilde{o}$ and o with respect to their maximal ideal topologies, and let $\tilde{\mathcal{U}}$ and $\mathcal{U}$ be the multiplicative groups defined by

$$\tilde{\mathcal{U}} := \{f \in \hat{\tilde{o}} : f(\tilde{P}_\infty) = 1\} \quad \text{and} \quad \mathcal{U} := \{f \in \hat{o} : f(P_\infty) = 1\}.$$

Since $\tilde{o} \cap \hat{o} = o$, it is easily seen that $\tilde{U}/U$ is isomorphic to $\tilde{\mathcal{U}}/\mathcal{U}$. Note that every element of $\tilde{\mathcal{U}}$ is a formal power series in s with constant term 1. The endomorphism $p \cdot \mathrm{id}_G$ on $\underline{\mathrm{Pic}}^0_{C/k}$ is transferred to the endomorphism ϕ on $\tilde{\mathcal{U}}/\mathcal{U}$ given by $f(s) \longmapsto (f(s))^p$.

Let $f(s)$ be an element of $\tilde{\mathcal{U}} - \mathcal{U}$ such that $f(s)^p \in \mathcal{U}$, and express $f(s)$ in the form; $f(s) = 1 + g(s)$ with $g(0) = 0$. Then $g(s) \notin \hat{o}$ and $g(s)^p \in \hat{o}$. Then, for every element λ of $k^\times$, $\lambda g(s) \notin \hat{o}$ and $(\lambda g(s))^p \in \hat{o}$. Consequently, $f_\lambda(s) := 1 + \lambda g(s) \in \tilde{\mathcal{U}} - \mathcal{U}$ for every $\lambda \neq 0$ and $(f_\lambda(s))^p \in \mathcal{U}$. This implies that the element of $\tilde{\mathcal{U}}/\mathcal{U}$ represented by $f(s)$ is connected to the point of origin (represented by 1 in $\tilde{\mathcal{U}}$) by an affine line contained in $\mathrm{Ker}\ \phi$. Therefore, $H(\bar{k})$ (=$\mathrm{Ker}\ \phi$) is connected. Q.E.D.

4.5.3.1. Remark. For a commutative connected unipotent k-group G, one or both of the kernels of $p \cdot id_G$ and the Verschiebung $V_G : G^{(p)} \longrightarrow G$ may fail to be geometrically connected. For example, let W_2 be the Witt vector group of dimension 2 and L the subgroup of W_2 given by $L = \{(0, \alpha) : \alpha \in k = \overline{k}, \alpha^p = \alpha\}$. L is isomorphic to Z/pZ. Let $G := W_2/L$. Then, G is a commutative connected unipotent k-group, and $Ker(V_G) \simeq G_a \times (Z/pZ)$, which is disconnected. Hence, $Ker(p \cdot id_G)$ is not connected, either.

4.5.4. PROPOSITION. With the notations of 4.5.2, the kernel of $\phi_0 : \underline{Pic}^0_{C'/k} \longrightarrow \underline{Pic}^0_{C/k}$ is geometrically connected.

Proof. We may assume that $\underline{Pic}^0_{C'/k} \neq \{0\}$. Then $\psi_0 : \underline{Pic}^0_{C/k} \otimes (f,k) \longrightarrow \underline{Pic}^0_{C'/k}$ is faithfully flat because $i'(X^{(p)}(k))$ and $i^{(p)}(X^{(p)}(k))$ generate dense subgroups in $\underline{Pic}^0_{C'/k}$ and $\underline{Pic}^0_{C/k} \otimes (f,k)$, respectively, and $i' = \psi_0 \circ i^{(p)}$. Since F_G is faithfully flat and $\phi_0 \circ \psi_0 \circ F_G$ is the "multiplication by p" endomorphism $p \cdot id_G$ on $G = \underline{Pic}^0_{C/k}$, it follows that $Ker\ \phi_0 = (\psi_0 \circ F_G)(Ker(p \cdot id_G))$. As $Ker(p \cdot id_G)$ is geometrically connected by 4.5.3, we conclude that $Ker(\phi_0)$ is geometrically connected. Q.E.D.

4.5.5. Our purpose now is to show that $\phi_0 : \underline{Pic}^0_{C'/k} \longrightarrow \underline{Pic}^0_{C/k}$ is a closed immersion. When $\underline{Pic}^0_{C'/k} = \{0\}$, this is obvious. When $\underline{Pic}^0_{C'/k} \neq \{0\}$, we have only to show that $Lie(\phi_0) : Lie(\underline{Pic}^0_{C'/k}) \longrightarrow Lie(\underline{Pic}^0_{C/k})$ is injective, since $Ker(\phi_0)$ is already known to be geometrically connected by virtue of 4.5.4. (Consult [3], [4] for material on Lie algebras employed here.) But

$\mathrm{Lie}(\underline{\mathrm{Pic}}^0_{C'/k}) = H^1(C', \mathcal{O}_{C'})$, $\mathrm{Lie}\,(\underline{\mathrm{Pic}}^0_{C/k}) = H^1(C, \mathcal{O}_C)$ and $\mathrm{Lie}(\phi_0)$ is identified with $\phi^* : H^1(C', \mathcal{O}_{C'}) \longrightarrow H^1(C, \mathcal{O}_C)$. Therefore we have only to show the next

LEMMA. *With the notations as above,* $\phi^* : H^1(C', \mathcal{O}_{C'}) \longrightarrow H^1(C, \mathcal{O}_C)$ *is injective.*

Proof. Since H^1 commutes with the base extension $k \hookrightarrow \bar{k}$, it suffices to prove the injectivity of $H^1(\bar{C}', \mathcal{O}_{C'}) \longrightarrow H^1(\bar{C}, \mathcal{O}_{\bar{C}})$, where $\bar{C} = C \otimes \bar{k}$, $\bar{C}' = C' \otimes \bar{k}$. But it is easy to see, just as in the proof of 4.0.5, that

$$H^1(\bar{C}, \mathcal{O}_{\bar{C}}) \simeq \tilde{o}_\infty/\bar{o}_\infty, \quad H^1(\bar{C}', \mathcal{O}_{\bar{C}'}) \simeq \tilde{o}'_\infty/\bar{o}'_\infty$$

where $\bar{o}_\infty = \bar{k} \otimes o_\infty$, $\bar{o}'_\infty = \bar{k} \otimes o'_\infty$ with unique places o_∞, o'_∞ at infinity of X, $X^{(p)}$, respectively; and $\tilde{o}_\infty$, $\tilde{o}'_\infty$ the normalizations of $\bar{o}_\infty$, $\bar{o}'_\infty$, respectively. As the mapping $\bar{\phi}^* : \tilde{o}'_\infty/\bar{o}'_\infty \longrightarrow \tilde{o}_\infty/\bar{o}_\infty$ is induced from the canonical mapping $(k,f) \otimes K \longrightarrow K$ given by $\xi \otimes a \longmapsto \xi a^p$ (cf. 0.3.1), it follows that $\bar{\phi}^*$ factors as $\tilde{o}'_\infty/\bar{o}'_\infty \xrightarrow{\sim} \tilde{o}_1/\bar{o}_1 \longrightarrow \tilde{o}_\infty/\bar{o}_\infty$, where $o_1 := o_\infty \cap k[K^p]$, $\bar{o}_1 := \bar{k} \otimes o_1$ and $\tilde{o}_1$:= the integral closure of $\bar{o}_1$, with $\tilde{o}_1/\bar{o}_1 \longrightarrow \tilde{o}_\infty/\bar{o}_\infty$ coming from the natural inclusion $o_1 \hookrightarrow o_\infty$. Left only to prove the injectivity of $\tilde{o}_1/\bar{o}_1 \longrightarrow \tilde{o}_\infty/\bar{o}_\infty$, i.e., $\tilde{o}_1 \cap \bar{o}_\infty \subseteq \bar{o}_1$. But if $\sum \xi_i \otimes y_i \in \bar{k} \otimes o_\infty$ is such that the y_i's are k-linearly independent, then to have also $\sum \xi_i \otimes y_i \in \bar{k} \otimes k[K^p]$ implies all $y_i \in o_\infty \cap k[K^p] = o_1$, because $k[K^p]$ is a regular extension of k. Thus,

$\sum \xi_i \otimes y_i \in \bar{k} \otimes o_1 = \bar{o}_1$. Q.E.D.

4.6. Summarizing the results in the preceding paragraphs that started with 4.5, one can state now the following theorem:

THEOREM. *In the situation of* 4.5.2, *the following hold*:

(a) $\phi_0 \cdot \psi_0 = V_G$ (= *the Verschiebung of* $\underline{\mathrm{Pic}}^0_{C/k}$), *and the k-homomorphism* ϕ_0 *is a closed immersion*;

(b) $\phi_0(\underline{\mathrm{Pic}}^0_{C'/k}) = p(\underline{\mathrm{Pic}}^0_{C/k})$, *the image of* $G := \underline{\mathrm{Pic}}^0_{C/k}$ *under the "multiplication by p" endomorphism* $p \cdot \mathrm{id}_G$.

COROLLARY 1. *The exponent of* $\underline{\mathrm{Pic}}^0_{C/k}$ *equals* $p^{\lambda'}$, *where* $\lambda' = \mathrm{ht}\, k(X)$.

Proof. Let $C^{(i)}$ be the normalization of $C^{[i]} := C \otimes (f^i, k)$ in its function field. By virtue of 0.3.2, $C^{(i)}$ is k-isomorphic to P^1_k if and only if C_i in the notation of 4.3 is $k^{p(-i)}$-isomorphic to P^1_k. The theorem above implies that $\underline{\mathrm{Pic}}^0_{C^{(i)}/k}$, identified with a k-subgroup scheme of $\underline{\mathrm{Pic}}^0_{C/k}$, is the image of the "multiplication by p^i" endomorphism $p^i \cdot \mathrm{id}_G$ of $G = \underline{\mathrm{Pic}}^0_{C/k}$. Since $\underline{\mathrm{Pic}}^0_{C(i)/k} = \{0\}$ if and only if C(i) is k-isomorphic to P^1, we deduce that the exponent of $\underline{\mathrm{Pic}}^0_{C/k}$ agrees with $p^{\lambda'}$, as asserted. Q.E.D.

COROLLARY 2. *With the notations of* 4.3.2, *the exponent of* $C^0(A)$ *is less than or equals* $p^{\lambda'}$, *where* $\lambda' = \mathrm{ht}(k(X))$; *the equality holds provided* X *has two k-rational points*.

Proof. By 4.3.2 and Corollary 1 above, $p^{\lambda'}$ annihilates $C^0(A)$. Assume that p^r is the exponent of $C^0(A)$, so $r \leq \lambda'$. Let P and Q be

distinct k-rational points of X, and let p and q be the prime ideals of A corresponding to P and Q, respectively. Let $p_r := p \cap A^{[r]}$ and $q_r := q \cap A^{[r]}$, where $A^{[r]} := A \otimes (f^r,k)$ (cf. Proof of 4.2.3). Then $p_rA = p^{p(r)}$ and $q_rA = q^{p(r)}$. Moreover, there exists an element ξ of $K := k(X)$ such that $(pq^{-1})^{p(r)} = \xi A$. We shall show that $\xi \in K^{[r]}$ and $p_rq_r^{-1} = \xi A^{[r]}$. In fact, put $\overline{A} := \overline{k} \otimes A = \overline{k}[t]$ and let $\overline{K} := \overline{k} \otimes K = \overline{k}(t)$. Then P and Q are given by $t = \alpha$ and $t = \beta$ with $\alpha, \beta \in \overline{k}$, respectively. Therefore, $pq^{-1} = ((t - \alpha)/(t - \beta))\overline{A}$. Hence $\xi = \gamma\,((t - \alpha)/(t - \beta))^{p(r)}$ with $\gamma \in \overline{k}$. This implies that $\xi \in K \cap \overline{K}^{[r]} = K^{[r]}$. Then, $p_rq_r^{-1}A = \xi A$ implies that $p_rq_r^{-1} = \xi A^{[r]}$. Since p_r and q_r correspond to k-rational points of $X^{[r]} := \operatorname{Spec} A^{[r]}$, $X^{[r]}$ is k-rational, which gives $r \geq \lambda'$. Taking the previous inequality $\lambda' \geq r$ into account, we get $r = \lambda'$. Q.E.D.

4.7. In this subsection, assuming that $k = k_s$ we shall determine explicitly $\underline{\mathrm{Pic}}^0_{C/k}$ for a k-form of A^1 of type: $y^2 = x^p + a$ with $a \in k$ and $a \notin k^p$, where $p > 2$. The curve is elliptic if $p = 3$, hyperelliptic if $p > 3$. The homogeneous form of the curve is

$$Y^2Z^{p-2} = X^p + aZ^p$$

where $x := X/Z$ and $y := Y/Z$. The singular point P_∞ of C dominates the point $(x,y) = (-\alpha,0)$, where $\alpha^p = a$. Let $u := X/Y$ and $v := Z/Y$. Then we get:

$$v^{p-2} = u^p + av^p \tag{7}$$

We know from the results of §2 that the k-normalization of the affine k-curve in the (u,v)-plane given by the equation (7) is a k-form X of A^1. The k-normal completion C of X is obtained by adjoining the local ring of the curve: $y^2 = x^p + a$ at $(x,y) = (-\alpha,0)$ to X.

Let $k' := k(\alpha)$, and let t be a parameter of $X \otimes k' = A^1_{k'}$ such that $v = t^p$ and $u + \alpha v = t^{p-2}$.

4.7.1. LEMMA. The affine algebra A of X is given by

$$A = k[t^p,\ t^{p-2}(1 - \alpha t^2),\ t^{p-4}(1 - \alpha t^2)^2,\ \ldots,\ t(1 - \alpha t^2)^{\ell}]$$

where $p = 2\ell + 1$.

Proof. Let $\eta_0 := t^p$ and $\eta_i := t^{p-2i}(1 - \alpha t^2)^i$ for $1 \le i \le \ell$. Then, by computation, one can show that

$$t = \eta_{\ell} + \ell\alpha\eta_{\ell-1} + \ldots + \binom{\ell}{i}\alpha^i\eta_{\ell-i} + \ldots + \ell\alpha^{\ell-1}\eta_1 + \alpha^{\ell}\eta_0.$$

Therefore, $k' \otimes A = k'[t]$. Since $k' \otimes A$ is faithfully flat over A, clearly A is k-normal. On the other hand, since $\eta_0 = v$ and $\eta_i = u^i v^{-i+1}$ $(1 \le i \le \ell)$, A contains the affine algebra of the curve (7) and is k-birationally equivalent to it. Therefore, A is the k-normalization of the affine algebra of the curve (7). Q.E.D.

4.7.2. LEMMA. In the above notations, $d\eta_1, \ldots, d\eta_{\ell}$ form a k-basis of $\omega_{C/k}$.

Proof. We have: $d\eta_i = -2it^{p-2i-1}(1 - \alpha t^2)^{i-1}dt$ for $1 \le i \le \ell$. Let $s := 1/t$. Then $d\eta_i = (2i(s^2 - \alpha)^{i-1}/s^{2\ell})ds$ for $1 \le i \le \ell$. Moreover,

the degree of the conductor of the normalization of $\bar{k} \otimes o_\infty$, which is equal to $\bar{k}[s]_{(s)}$, to $\bar{k} \otimes o_\infty$ is 2ℓ. Since the maximal ideal of $\bar{k} \otimes o_\infty$ is generated by t^2 and $t^{2\ell+1}$, it is not hard to show that $\mathrm{Res}_{\tilde{P}_\infty}(f d\eta_i) = 0$ for every $1 \le i \le \ell$ and for every $f \in \bar{k} \otimes o_\infty$, where $\tilde{P}_\infty$ denotes the point of P^1_k lying over P_∞. Therefore, $d\eta_1, \ldots, d\eta_\ell \in \omega_{C/k}$. It is clear that they are linearly independent over k and generate $\omega_{C/k}$. Q.E.D.

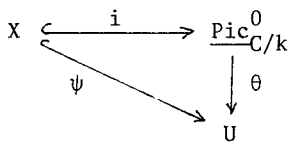
4.7.3. Let U be the unipotent k-group defined as

$$\bar{U} := \mathrm{Spec}(k[Y_0, Y_1, \ldots, Y_\ell]/(Y_0 - \textstyle\sum_{i=0} \binom{\ell}{i} a^i Y^p_{\ell-i})) \quad \text{where}$$

$$p = 2\ell + 1,$$

endowed with the group law defined by the following comultiplication $\Delta : \Delta(Y_i) := Y_i \otimes 1 + 1 \otimes Y_i$ for $0 \le i \le \ell$. Define a k-morphism $\psi : X \longrightarrow U$ by the homomorphism of k-algebras $\psi^*(Y_i) := \eta_i$. ψ is obviously an imbedding.

4.7.3.1. LEMMA. *There exists a k-homomorphism of k-group schemes* $\theta : \underline{\mathrm{Pic}}^0_{C/k} \longrightarrow U$ *such that the following diagram commutes:*



Proof. Take the k-rational point P_0 used to define i in 4.0 to be the point $(\eta_0, \eta_1, \ldots, \eta_\ell) = (0, 0, \ldots, 0)$. Let $\sum n_j P_j$ be a divisor on

X representing a point $\sum n_j i(P_j)$ in $\mathrm{Pic}^0_{C/k}$. Define $\theta(\sum n_j i(P_j)) := \sum n_j \psi(P_j)$. We are going to show the following two facts:

(a) Let $\overline{X} := X \otimes \overline{k}$, $\overline{C} := C \otimes \overline{k}$ and $\overline{o} := \mathcal{O}_{\overline{P}_\infty, \overline{C}}$. For each element f of $\overline{o}^\times$, write $(f) = \sum n_j P_j$ with $P_j \in \overline{X}$. Then, $\sum n_j \psi(P_j) = 0$.

(b) Let Q be any k-rational point on X. Then $\theta(i(Q)) = \psi(Q)$ is k-rational.

The assertion (a) implies that $\theta_{\overline{k}} : \underline{\mathrm{Pic}}^0_{C/k} \otimes \overline{k} \longrightarrow U \otimes \overline{k}$ is a homomorphism of algebraic groups defined over $\overline{k}$, in view of the fact that $\underline{\mathrm{Pic}}^0_{C/k} \otimes \overline{k}$ is the generalized Jacobian variety J' of P^1_k with equivalence relation defined by $\overline{o}$ (cf. 4.0.5) and that J' has the universal mapping property as described in [13]. Since $i(X(k))$ generates a dense subgroup in $\underline{\mathrm{Pic}}^0_{C/k}$, the assertion (b) implies that $\theta_{\overline{k}}$ is in fact defined over k.

Proof of the assertion (a): The proof consists of three steps: (I) Take a parameter of $X_{\overline{k}}$ as indicated in 4.7, and let $s := 1/t$. Then $f = h/g$ with $g,h \in \overline{k}[s^2, s^p]$ such that $g(0) \neq 0$ and $h(0) \neq 0$. Let $d := \deg_s h$, $d' := \deg_s g$, and set $h_1 := t^d h(1/g)$, $g_1 := t^{d'} g(1/t)$. Then $(f) = (h_1)_0 - (g_1)_0 + (d' - d)P_0$, where $(h_1)_0$ and $(g_1)_0$ are the divisors of zeroes of h_1 and g_1, respectively. Since $\psi(P_0) = 0$, in order to show that $\psi((f)) = 0$ it suffices to show that $\psi((f)_0) = 0$ for every polynomial f of degree d in t such that $f(0) \neq 0$ and $s^d f(1/s) \in \overline{k}[s^2, s^p]$. On the other hand, it is easy to show that $\psi((1 - t^p)_0) = 0$. Hence, we may assume that d is even, replacing f by $(1 - t^p)f$ when d is odd. Moreover, as one can readily verify, f is of the form:

$$f = c_0 t^d + c_2 t^{d-2} + \ldots + c_{2\ell-2} t^{d-2\ell+2} + c_{2\ell} t^{d-2\ell} +$$

$$c_{2\ell+1} t^{d-(2\ell+1)} + \ldots + c_d,$$

where the coefficients of t^{d-2i+1} $(1 \le i \le \ell)$ are all zero.

(II) Write f in the form: $f = c_0(t - \beta_1)\ldots(t - \beta_d)$ with $\beta_1, \ldots, \beta_d \in \overline{k}$. We shall show that $\beta_1^n + \beta_2^n + \ldots + \beta_d^n = 0$ for $n = 2i - 1$ $(1 \le i \le \ell)$. Indeed, $(t - \beta_1^n)\ldots(t - \beta_d^n) = t^d - (\beta_1^n + \beta_2^n + \ldots + \beta_d^n)t^{d-1}$ + (terms of degree $< d - 1$). Let $t := u^n$. Since $n < p = 2\ell + 1$, we have

$$\prod_{j=1}^{d} (t - \beta_j^n) = \prod_{i=0}^{n-1} \prod_{j=1}^{d} (u - \zeta^i \beta_j)$$

$$= \left(\prod_{j=1}^{d} (u - \beta_j)\right)\left(\prod_{j=1}^{d} (u - \zeta\beta_j)\right) \ldots \left(\prod_{j=1}^{d} (u - \zeta^{n-1}\beta_j)\right) \qquad (8)$$

where ζ is a primitive n-th root of unity. For every $0 \le i \le n - 1$, the coefficients of $u^{d-1}, u^{d-3}, \ldots, u^{d-2\ell+1}$ in $\prod_{j=1}^{d} (u - \zeta^i \beta_j)$ are zero. Moreover, if $(d - 1)n$ is a sum of n positive integers $\le d$, $(d - 1)n = m_1 + \ldots + m_n$, then every m_i $(1 \le i \le n)$ should be $\ge d - 2\ell + 1$. Consequently, if the monomial of degree $(d - 1)n$ on the right hand side of (8) is nonzero, it is a sum of products of n-monomials of even degree. This is absurd because $(d - 1)n$ is odd. Therefore, $\beta_1^n + \beta_2^n + \ldots + \beta_d^n = 0$ for every $n = 2i + 1$ $(1 \le i \le \ell)$.

(III) $\psi((f)_0) = \left(\sum_{j=1}^{d} \eta_0(\beta_j), \sum_{j=1}^{d} \eta_1(\beta_j), \ldots, \sum_{j=1}^{d} \eta_\ell(\beta_j)\right)$, where $\eta_i(\beta_j) = \beta_j^{p-2i}(1 - \alpha\beta_j^2)^i$ for $0 \le i \le \ell$. Since η_i is a linear combination of $t^{2(\ell-i)+1}, t^{2(\ell-i+1)+1}, \ldots, t^p$, we know that $\sum_{j=1}^{d} \eta_i(\beta_j) = 0$ for $0 \le i \le \ell$. This proves assertion (a).

Proof of the assertion (b): Simply note that, if Q is a k-rational point, u and v have k-rational values. So do all η_i's. Thus it is obvious that $\psi(Q)$ is k-rational.

Proof of 4.7.3.1 is now complete.

4.7.3.2. LEMMA. The kernel of the k-homomorphism θ defined in 4.7.3.1 is geometrically connected.

Proof. The assertion will be proved by explicitly computing $\underline{\mathrm{Pic}}^0_{C/k}(k)$. Let $\alpha^p = a$, for $\alpha \in \overline{k}$ and $k' := k(\alpha)$. Let $A' := k' \otimes A$ and let K' be the field of quotients of A'. Then $A' = k'[t]$ and $K' = k' \otimes K = k'(t)$, K being the field of quotients of A. There exists a unique k-rational derivation D on k' such that $D(\alpha) = 1$ and $D^p = 0$. Extend D to a K-trivial derivation on K' by defining $D(c \otimes f) := D(c) \otimes f$ for $c \in k'$ and $f \in K$. Then it is easy to ascertain that $D(t) = -(1/2)t^3$, $D(A') \subseteq A'$, K'^D (:= the set of D-invariant elements of K') $= K$, and $A'^D = A$. By KMT - 6.3.1, there is an exact sequence of groups

$$0 \longrightarrow L/L_0 \longrightarrow C(A) \longrightarrow C(A')$$

where $L = \{D(f)/f \in A' : f \in K' - \{0\}\}$ and $L_0 = \{D(u)/u : u \in A'^{\times}\}$ Since $C(A') = (0)$, it follows that $C(A) \simeq L/L_0$.

Let us compute L. Since k' is separably closed, any irreducible monic polynomial in $k'[t]$ is of the form $t^{p(n)} - \beta$ with $\beta \in k'$. Hence L is generated by elements of the form $D(t^{p(n)} - \beta)/(t^{p(n)} - \beta)$ and $D(\gamma)/\gamma$ with $\gamma \in k'$. It is clear that, for $n > 0$,

$D(t^{p(n)} - \beta)/(t^{p(n)} - \beta) \notin A'$. Therefore L is generated by elements of the form $D(t - \beta)/(t - \beta)$ and $D(\gamma)/\gamma$. But $D(t - \beta) = -(1/2)(t^3 + 2D(\beta))$. Thus, $D(t - \beta)/(t - \beta) \in A'$ if and only if $2D(\beta) + \beta^3 = 0$. For simplicity's sake, let us denote $D^i(\beta)$ by $\beta^{(i)}$. Then, it is easy to verify that

$$2^i\beta^{(i)} = (-1)^i\ 1\ 3 \ldots (2i - 1)\beta^{2i+1}.$$

Hence, for $i = \ell = (p - 1)/2$, we have

$$\beta^{(\ell)} = (-1)^\ell\ 1\ 3 \ldots (2\ell - 1)2^{-\ell}\beta^p = (\ell!)\beta^p.$$

This implies that, if we express $\beta \in k'$ in the form $\beta = d_0 + d_1\alpha + \ldots + d_{p-1}\alpha^{p-1}$ with $d_0, \ldots, d_{p-1} \in k$, then $d_{\ell+1} = \ldots = d_{p-1} = 0$. Therefore, we may express β in the form

$$\beta = c_\ell + \ell c_{\ell-1}\alpha + \ldots + \binom{\ell}{i} c_{\ell-i}\alpha^i + \ldots + c_0\alpha^\ell$$

with $c_0, \ldots, c_\ell \in k$. Since $\beta^{(\ell)} = (\ell!)c_0$, we have $c_0 = \beta^p$, i.e.,

$$c_0 = \sum_{i=0}^{\ell} \binom{\ell}{i} c_{\ell-i}^p a^i.$$

Now, mapping $D(t - \beta)/(t - \beta)$ to $(c_0, c_1, \ldots, c_\ell)$ we obtain a point in U.

On the other hand, if $\beta^3 + 2D(\beta) = 0$ then $D(t - \beta)/(t - \beta) = -(1/2)(t^2 + \beta t + \beta^2)$. Since $D(\beta)/\beta = -\beta^2/2 \in L_0$, L/L_0 is generated by elements of the form $-(1/2)(t^2 + \beta t)$ with $\beta^3 + 2D(\beta) = 0$. Moreover, since $-(1/2)t^2 = D(t)/t$ corresponds to the rational point on X given by $(u,v) = (0,0)$, we know that $C^0(A)$ is generated by elements of the form $-(1/2)(\beta t)$ with $\beta \in k'$ subject to

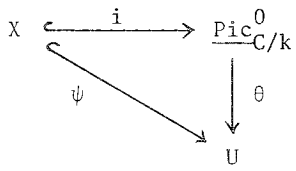
$\beta^3 + 2D(\beta) = 0$. Evidently, the addition of such elements is given by $-(1/2)(\beta t) - (1/2)(\gamma t) = -(1/2)(\beta + \gamma)t$. Now $\theta : \underline{\mathrm{Pic}}^0_{C/k} \longrightarrow U$, restricted on $\underline{\mathrm{Pic}}^0_{C/k}(k) \simeq C^0(A)$, is given by

$$\theta(-(1/2)(\beta t)) = (c_0, c_1, \ldots, c_\ell).$$

It is straightforward to check that θ is injective on $C^0(A)$. Therefore $\mathrm{Ker}(\theta)(k) = (0)$. Since k is separably closed, $\mathrm{Ker}(\theta)$ is geometrically connected. Q.E.D.

4.7.4. THEOREM. *The unipotent k-group scheme U defined in 4.7.3 is the connected Picard scheme* $\underline{\mathrm{Pic}}^0_{C/k}$.

Proof. By 4.7.3.1 we have a commutative diagram of k-morphisms



where both i and ψ are closed immersions and θ is a k-homomorphism. Let Ω and Ω_U be the spaces of invariant differentials on $\underline{\mathrm{Pic}}^0_{C/k}$ and U, respectively. By 4.0.6.1 we have an isomorphism $i^* : \Omega \xrightarrow{\sim} \omega_{C/k}$, and by 4.7.2 another isomorphism $\psi^* : \Omega_U \xrightarrow{\sim} \omega_{C/k}$. Since $\psi^* = i^* \cdot \theta^*$, we get an isomorphism $\theta^* : \Omega_U \xrightarrow{\sim} \Omega$. Therefore we have an isomorphism $\mathrm{Lie}(\theta) : \mathrm{Lie}(\underline{\mathrm{Pic}}^0_{C/k}) \xrightarrow{\sim} \mathrm{Lie}(U)$. Taking 4.7.3.2 and its proof into account, we conclude that θ is an isomorphism. Q.E.D.

4.7.4.1. COROLLARY. *The Picard scheme* $\underline{\mathrm{Pic}}^0_{C/k}$ *is obtained as an extension*

of the vector group $G_a^{\ell-1}$ by a Russell type k-group $G := \mathrm{Spec}(k[x,y]/(y^p - x + a^{\ell}x^p))$:

$$0 \longrightarrow G \xrightarrow{\tau} \underline{\mathrm{Pic}}^0_{C/k} \xrightarrow{\sigma} G_a^{\ell-1} \longrightarrow 0.$$

Proof. Having identified $\underline{\mathrm{Pic}}^0_{C/k}$ with U, one can give to the homomorphisms σ and τ explicit expressions in terms of their cohomomorphisms σ^* and τ^* as follows:

$\sigma^*(t_i) = Y_i$, if $t_1, \ldots, t_{\ell-1}$ are generating parameters of $G_a^{\ell-1}$;

$\tau^*(Y_0) = x$, $\tau^*(Y_{\ell}) = y$, and $\tau^*(Y_i) = 0$ for $1 \leq i \leq \ell - 1$.

Q.E.D.

References

[1] Artin, E.: Algebraic Numbers and Algebraic Functions. New York: Gordon and Breach 1967.

[2] Chevalley, C.: Introduction to the Theory of Algebraic Functions of One Variable. Amer. Math. Soc. Mathematical Surveys 6. New York 1951.

[3] Demazure, M., Gabriel, P.: Groupes Algébriques, Tome I. Paris-Amsterdam: Masson et Cie. - North Holland Publ. Co. 1970.

(SGA 3) [4] Demazure, M., Grothendieck, A.: Schémas en Groupes. Lecture Notes in Mathematics 151. Berlin-Heidelberg-New York: Springer 1970.

[5] Fulton, W.: Algebraic Curves. An introduction to algebraic geometry. Mathematics Lecture Note Series. New York - Amsterdam: W. A. Benjamin, Inc. 1969.

(EGA) [6] Grothendieck, A., Dieudonné, J.: Éléments de Géométrie Algébrique. Publ. Math. I.H.E.S. 20 ff.

[7] Hartshorne, R.: Residues and Duality. Lecture Notes in Mathematics 20. Berlin-Heidelberg-New York: Springer 1966.

(KMT) [8] Kambayashi, T., Miyanishi, T., Takeuchi, M.: Unipotent Algebraic Groups. Lecture Notes in Mathematics 414. Berlin - Heidelberg-New York: Springer 1974.

[9] Kambayashi, T.: On the absence of nontrivial separable forms of the affine plane. J. Algebra 35(1975), 449-456.

[10] Queen, C.: Non-conservative function fields of genus one, I. Arch. Math. (Basel) 2, 612-623 (1971).

[11] Rosenlicht, M.: Equivalence relations on algebraic curves. Ann. Math. 59, 169-191 (1952).

[12] Rosenlicht, M.: Generalized Jacobian varieties. Ann. Math. 59, 505-530 (1954).

[13] Rosenlicht, M.: A universal mapping property of generalized Jacobian varieties. Ann. Math. 60, 80-88 (1957).

[14] Rosenlicht, M.: Automorphisms of function fields. Trans. Amer. Math. Soc. 79 (1955), 1-11.

[15] Rosenlicht, M.: Some rationality questions on algebraic groups. Annali Mat. Pura Appl. (4), 43 (1957), 25-50.

[16] Rosenlicht, M.: Questions of rationality for solvable algebraic groups over nonperfect fields. Annali Mat. Pura Appl. (4), 61 (1963), 97-120.

[17] Russell, P.: Forms of the affine line and its additive group. Pacific J. Math. 32, 527-539 (1970).

[18] Seidenberg, A.: Elements of the Theory of Algebraic Curves. Reading, Mass.: Addison-Wesley 1968.

[19] Samuel, P.: Méthodes d'Algèbre Abstraite en Géométrie Algébrique. Berlin-Heidelberg-New York: Springer 1967.

[20] Serre, J.-P.: Groupes Algébriques et Corps de Classes. Paris: Hermann 1959.

[21] Serre, J.-P.: Cohomologie Galoisienne. Lecture Notes in Mathematics 5. Berlin-Heidelberg-New York: Springer-Verlag 1965.

[22] Tate, J.: Genus change in inseparable extensions of function fields. Proc. Amer. Math. Soc. 3, 400-406 (1952).

LECTURES IN MATHEMATICS, KYOTO UNIVERSITY

No. 1	Peterson, F. P.—Lectures in Cobordism Theory	$5.00
No. 2	Kubota, T.—On Automorphic Functions and the Reciprocity Law in a Number Field	$5.00
No. 3	Maruyama, M.—On Classification of Ruled Surfaces	$5.00
No. 4	Monsky, P.—p-adic Analysis and Zeta Functions	$5.00
No. 5	Nagata, M.—On Automorphism Group of k[x, y]	$5.00
No. 6	Araki, S.—Typical Formal Groups in Complex Cobordism and K-Theory	$5.00
No. 7	Shin'ya, H.—Spherical Functions and Spherical Matrix Functions on Locally Compacts Groups	$5.00
No. 8	Saito, H.—Automorphic forms and Algebraic Extensions of Number Fields	$7.00
No. 9	Tanaka, N.—A Differential Geometric Study on Strongly Pseudo-Convex Manifolds	$7.00

Printed by Tokyo Press Co., Ltd., Tokyo, Japan

Printed in Japan